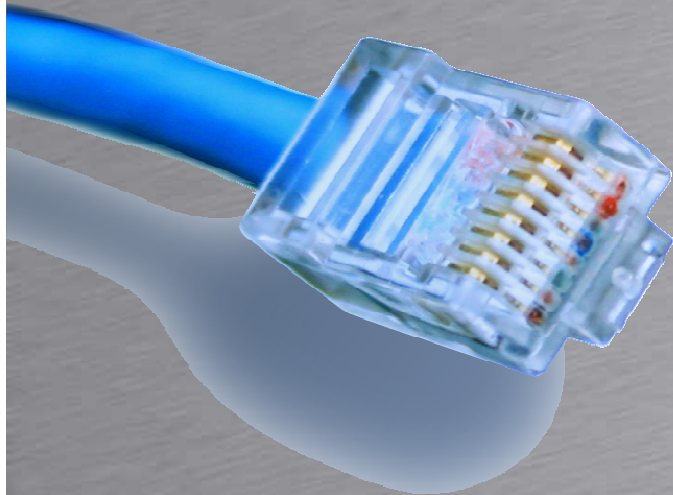


Sikkerhed

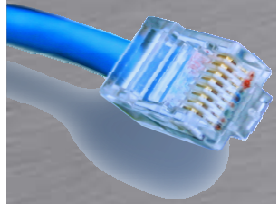


HOUSE OF
TECHNOLOGY



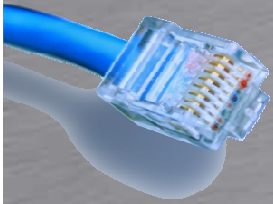
- en del af **mercantec⁺**

Rasmus Elmholt V1.0



Password

- Alle passwords på systemet er krypteret
 - Nogle med symetrisk kryptering(pas på)
 - Nogle mad SHA1 Hashing
- Skal bruge change-of-case
 - Set system login password minimum-change <tal>
- Password længde
 - Set system login password minimum-length <tal>

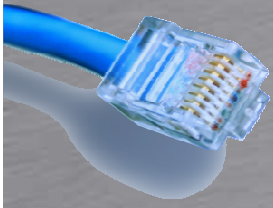


Root login



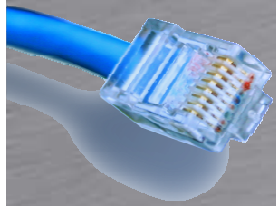
- Man kan forhindre root brugeren i at logge ind.
 - Set service ssh root-login deny
- Bruge SSH nøgler som authentication

```
root-authentication {  
    encrypted-password "$1$NnMs9VIQ$76Zkp141q5jFw1KBYhFpu/"; ## SECRET-DATA  
    ssh-dsa "ssh-dss  
AAAAB3NzaC1kc3MAAACBAILtxt6q2NKLUK+5SuOfnubxgTZ3+Ho4jpaun/JgG0cAUeyJXurhm/DOk  
HE1Hc/wFI8NApIgt9ur+SqPf6j6MNZwMgCOQuecQ1ad2kBeh+9RkNqe1FQYnxltU0JjX+9q2xbFL9  
xeOBsTolh4ZthLy/nfFkAaEGaWj7BjOn8BJvMvAAAAFQDnKGG0/7CHGBEyKoECQ/YpxFLQFwAAAIB  
FvOW3f/3mDBgf/LYp5MJqofqT+kFzxxkvYhhQa1FYsyopra393DbGpWe6JycXHOMJ+ZWWnEUAS4H  
mql/5zf3il9qYV9Y48WuitGXTPq9+zjhgQZGcheIBttXpfsk9croluxifyLQlMGspLmWxtfBwFrMh  
8/hmjbMh0VghWgx+AAAAIEAgGt+MhFZSDX3pwZRqlVtBCX5pkPMv4SMeeAf1vfPka5YG3oKVBwLXk  
SHrvTZQ7VLNjrM8I8KOKrqH4gCdWc2/HF74VsDRmo5mxwosNpSMycOsvBRO5fci2ze5mdOe9H7HZx  
ApGfE/68dzbQVqUbmQbt03JZlAJX1Z9SiOMf6TTM= dsa-key-20111110"; ## SECRET-DATA  
}
```



Login

- Hvem er logget ind?
 - Show system users
- Kick bruger
 - Request system logout <bruger>
- Indbygget Chat
 - Request message all message
"Slukker nu"



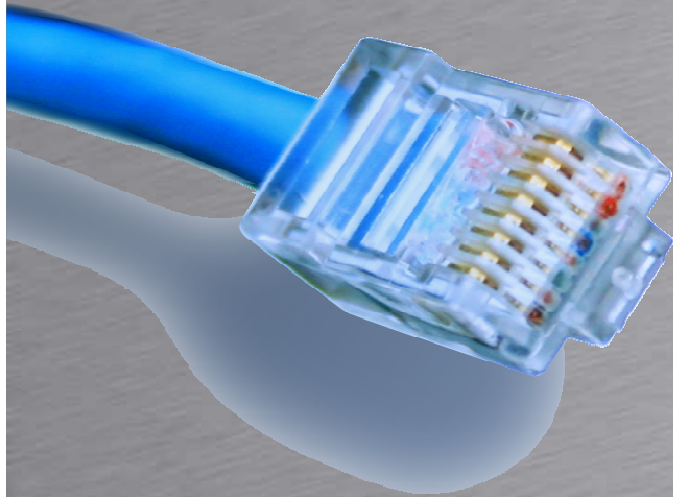
Konfiguration

- Hvem konfigurer nu?

```
[edit]
root@SRX210# status
Users currently editing the configuration:
  root terminal u0 (pid 1075) on since 2011-11-10 19:37:08 UTC
[edit]
```

- Configure exclusive
- Configure private
- Exit configuration-mode

Firewall

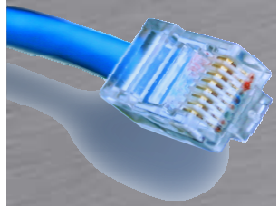


HOUSE OF
TECHNOLOGY



- en del af **mercantec⁺**

Firewall Filtre

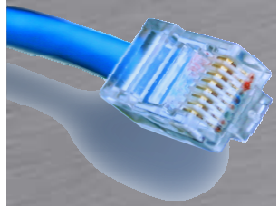


Firewall Filters

- Firewall filtre bruges til at bestemme hvad er kommer ind og ud af et interface.
 - Kan matche på de fleste header felter
 - Numeriske områder
 - Adresser
 - Bit felter
 - Laver bit matching(forklar)

```
+ Internet Protocol, Src: 10.1.4.16 (10.1.4.16), Dst: 8.8.8.8 (8.8.8.8)
+ User Datagram Protocol, Src Port: 60322 (60322), Dst Port: domain (53)
+ Domain Name System (query)
```

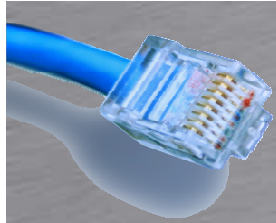
Øhh. Lav commit check når man leger med FW



Firewall Filters

- Terminating actions:
 - accept
 - reject
 - discard
- Flow Control
 - next term
- Actions modifiers
 - count, log, syslog
 - forwarding-class
 - policers

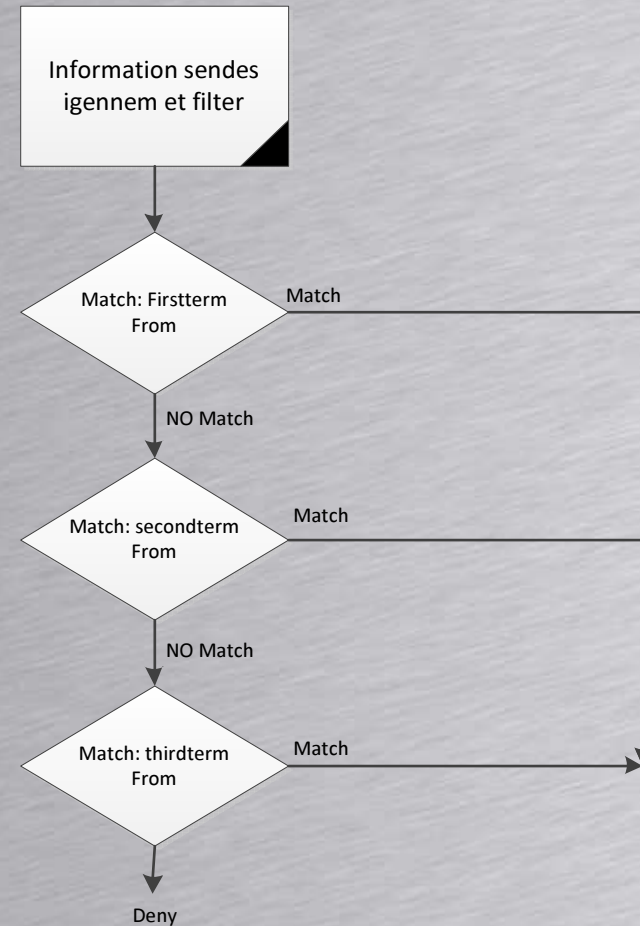
Alt hvad der ikke bliver tilladt er implicit deny

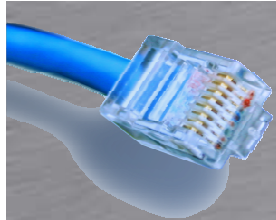


Firewall Filters

- Eksempel

```
[edit firewall family inet]
root@SRX210# show
filter filter-in {
  term block-source {
    from {
      source-address {
        10.0.0.0/24;
      }
    }
    then {
      count spoof-log;
      discard;
    }
  }
  term accept-other {
    then accept;
  }
}
```

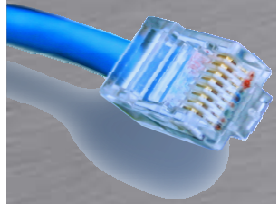




Firewall Filters

- Eksempel
 - Filter og protokol familie skal passe

```
[edit interfaces fe-0/0/4 unit 0]  
root@SRX210# show  
family inet {  
    filter {  
        input filter-in;  
    }  
}
```



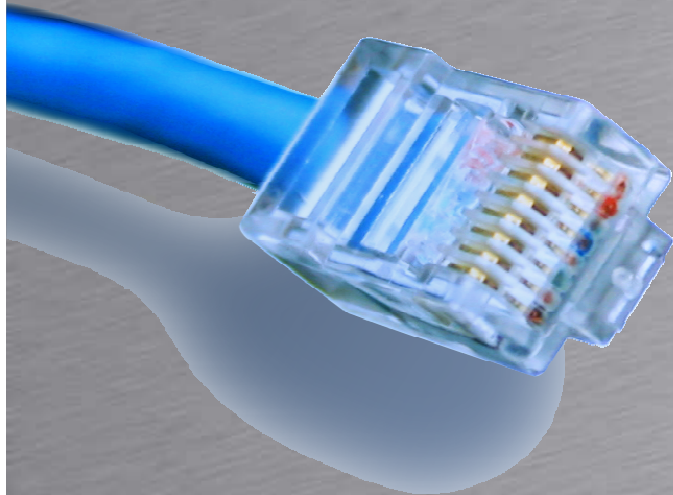
Policing



- Eksempel

```
[edit firewall]
root@SRX210# show
policer TIL-KUNDE {
    if-exceeding {
        bandwidth-limit 10m;
        burst-size-limit 100k;
    }
    then discard;
}
filter KUNDE-UD {
    term police {
        then {
            policer TIL-KUNDE;
            accept;
        }
    }
}
```

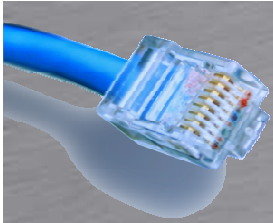
Device Hardening



HOUSE OF
TECHNOLOGY



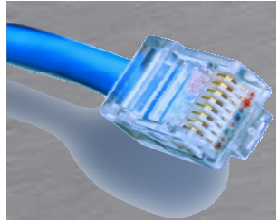
- en del af **mercantec⁺**



Terminal Sikkerhed

- Firewall politik for SSH/Telnet adgang
 - Alt trafik til RE går igennem Lo0 uanset hvilket fysisk interface det kommer fra.
 - Adgangs filter skal sættes på Lo0

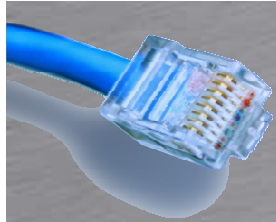
```
interfaces {  
  lo0 {  
    unit 0 {  
      family inet {  
        filter {  
          input-list SSH-ACCESS;  
        }  
      }  
    }  
  }  
}
```



Terminal Sikkerhed

- Firewall filter - Eksempel

```
root@SRX210# show firewall
filter SSH-ACCESS {
  term access-ssh {
    from {
      source-address {
        192.168.146.0/24;
      }
      protocol tcp;
      destination-port ssh;
    }
    then accept;
  }
  term deny-other {
    then {
      count SSH-DENY-COUNTER;
      reject;
    }
  }
}
```



Terminal Sikkerhed

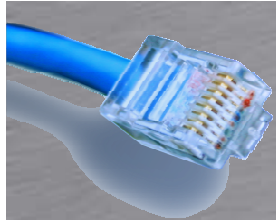
- Firewall filter – Show counter

```
root@SRX210> show firewall counter filter SSH-ACCESS SSH-DENY-COUNTER
```

```
Filter: SSH-ACCESS
```

```
Counters:
```

Name	Bytes	Packets
SSH-DENY-COUNTER	0	0



Terminal Sikkerhed

HOUSE OF
TECHNOLOGY



an ahl of merconter⁺

- Policing - Eksempel

```
[edit firewall]
root@SRX210# show
policer SSH-POLICER {
    if-exceeding {
        bandwidth-limit 512k;
        burst-size-limit 25k;
    }
    then discard;
}
filter SSH-ACCESS {
    term access-ssh {
        from {
            <output omitted>
        }
        then {
            policer SSH-POLICER;
            accept;
            <output omitted>
        }
    }
}
```