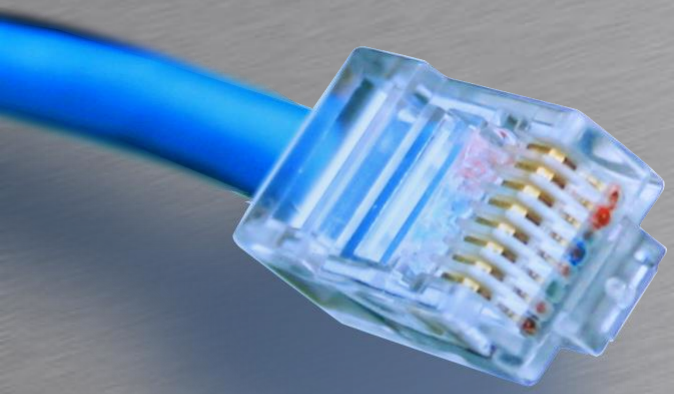
Sikkerhed



HOUSE OF TECHNOLOGY

– en del af mercantec

Rasmus Elmholt V1.0

Terminal Sikkerhed

HOUSE OF TECHNOLOGY
– en del af mercantec

- Ønsker man ikke adgang via Consol
  - `set system ports console disable`
- Skal root ikke kunne logge ind via Consol
  - `set system ports console insecure`
- Auto logout når Consol kabel fjernes
  - `set system ports console log-out-on-disconnect`

Password

HOUSE OF TECHNOLOGY
– en del af mercantec+

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

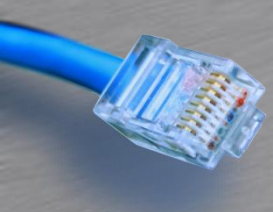
Root login

HOUSE OF TECHNOLOGY

– en del af mercantec+

- 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/JgGOcAUeyJXurhm/DOk
HE1Hc/wFI8NApIgT9ur+SqPf6j6MNZwMgCOQuecQ1ad2kBeh+9RkNqe1FQYnxltU0JjX+9q2xbFL9
xeOBsTolh4ZthLy/nfFkAaEGaWj7BjOn8BJvMvAAAAFQDnKGGO/7CHGBEyKoECQ/YpxFLQFwAAAIB
FvOW3f/3mDBgf/LYp5MJqofqT+kFzxkkvYhhQa1FYsyopra393DbGpWe6JycXHOMJ+ZWWnEUAZS4H
mql/5zf3il9qYV9Y48WuiTGXTpq9+zjhgQZGcheIBttXpfsk9cro1uxifyLQlMGspLmWxtfBwFrMh
8/hmjbMh0VghWgx+AAAAIEAgGt+MhFZSDX3pwZRqlVtBCX5pkPMv4SMeeAf1vfPka5YG3oKVBwLXk
SHrvTZQ7VLNJrM8I8KOKrqH4gCdWc2/HF74VsDRmo5mxwosNpSMycOsvBRO5fci2zE5mdOe9H7HZx
ApGfE/68dzbQVqUbmQbt03JZlAJX1Z9SiOMf6TTM= dsa-key-20111110"; ## SECRET-DATA
}
```



SSH

HOUSE OF TECHNOLOGY
– en del af mercantec

- Man kan definere hvor mange login forsøg der må laves i sekundet
  - `set system services ssh rate-limit`
- SSHv2

```
[edit]
root@SRX240# set system services ssh ?
Possible completions:
  <[Enter]>            Execute this command
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  connection-limit     Maximum number of allowed connections (1..5)
+ protocol-version     Specify ssh protocol versions supported
  rate-limit           Maximum number of connections per minute (1..5)
  root-login           Configure root access via ssh
```

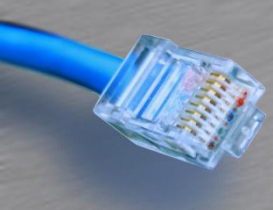
Login

HOUSE OF TECHNOLOGY

– en del af mercantec

- Login Retry blocking

```
[edit]
root@SRX240# set system login retry-options ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except   Don't inherit configuration data from these groups
  backoff-factor        Delay factor after 'backoff-threshold' password failures
  backoff-threshold     Number of password failures before delay is introduced
  minimum-time          Minimum total connection time if all attempts fail
  tries-before-disconnect  Number of times user is allowed to try password
```



Login

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Hvem er logget ind?
  - `Show system users`
- Kick bruger
  - `Request system logout`
- Indbygget Chat
  - `Request message all message "Slukker nu"`
- Auto logout af idle bruger
  - `set system login class super-user-local idle-timeout 10`

Konfiguration

HOUSE OF TECHNOLOGY

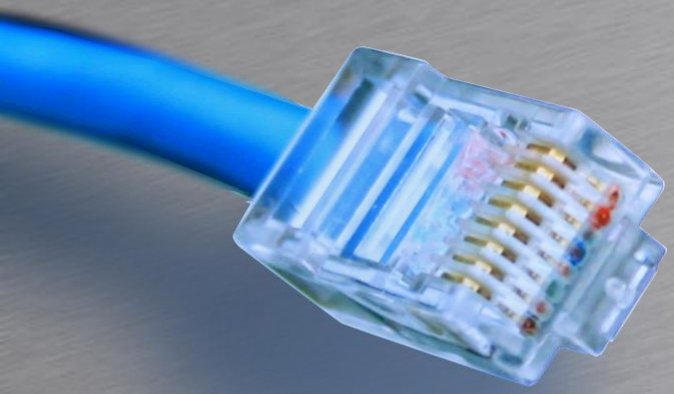
– en del af mercantec+

- 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

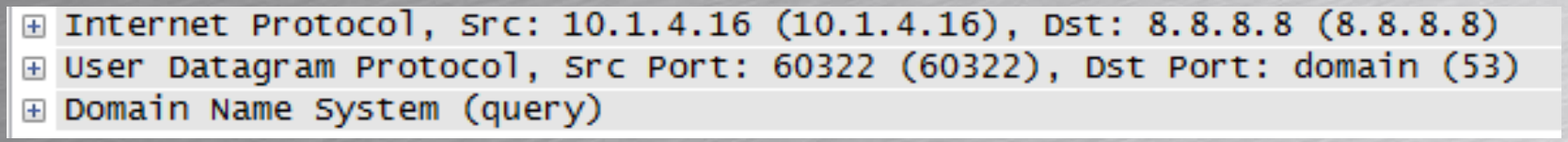
– en del af mercantec

Firewall Filtre

Firewall Filters

HOUSE OF TECHNOLOGY – en del af mercantec

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



Øhh. Lav commit check/confirm når man leger med FW

Firewall Filters

HOUSE OF TECHNOLOGY
– en del af mercantec+

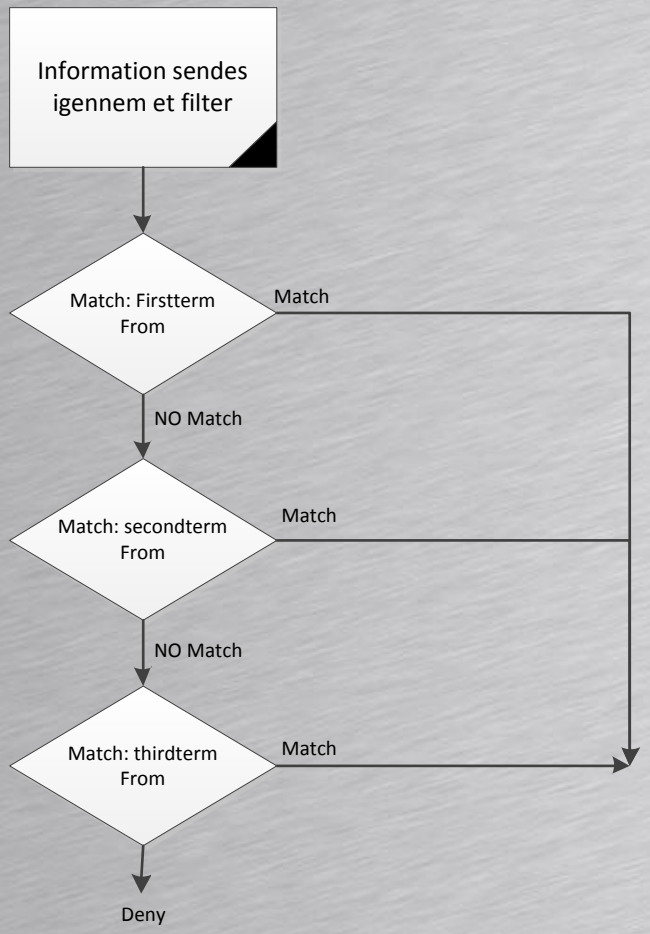
- Terminating actions:
  - accept
  - reject
  - discard
- Flow Control
  - next term
- Actions modifiers
  - count, log, syslog
  - forwarding-class
  - policers

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

HOUSE OF TECHNOLOGY

– en del af mercantec+

- 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

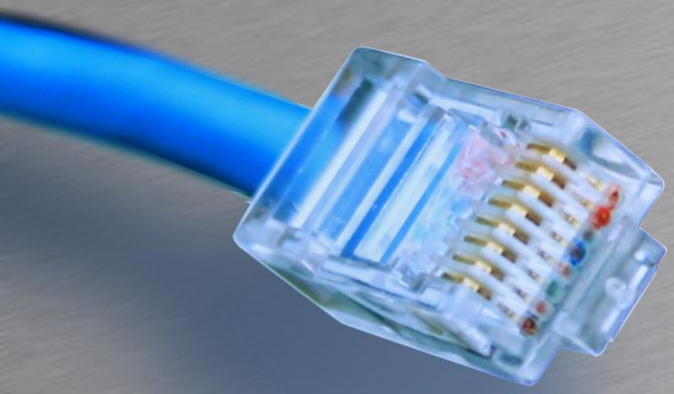
HOUSE OF TECHNOLOGY

– en del af mercantec+

- 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

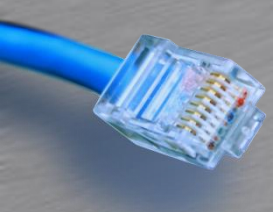
– en del af mercantec+

Terminal Sikkerhed

HOUSE OF TECHNOLOGY – en del af mercantec

- 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

HOUSE OF TECHNOLOGY – en del af mercantec

- 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;
        }
    }
```

Hvad med Routing Protokoller??

Terminal Sikkerhed

HOUSE OF TECHNOLOGY

– en del af mercantec

- 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

– en del af mercantec

- 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>
```

Bruger policing

HOUSE OF TECHNOLOGY – en del af mercantec

- Policing - Eksempel

```
[edit]
root@SRX07# show firewall
policer KUNDE_IND {
    if-exceeding {
        bandwidth-limit 10m;
        burst-size-limit 500k;
    }
    then discard;
}
filter KUNDE-MAKS {
    term 1 {
        then {
            policer KUNDE_IND;
            accept;
        }
    }
}
```

Maks burst size = hastighed * burst tid/8

Burst tid bør ikke være under 5ms

Terminal Sikkerhed

HOUSE OF TECHNOLOGY

– en del af mercantec

- Policing - Eksempel

```
[edit]
root@SRX07# show interfaces ge-0/0/0
unit 0 {
    family inet {
        filter {
            input KUNDE-MAKS;
        }
        dhcp;
    }
}
```