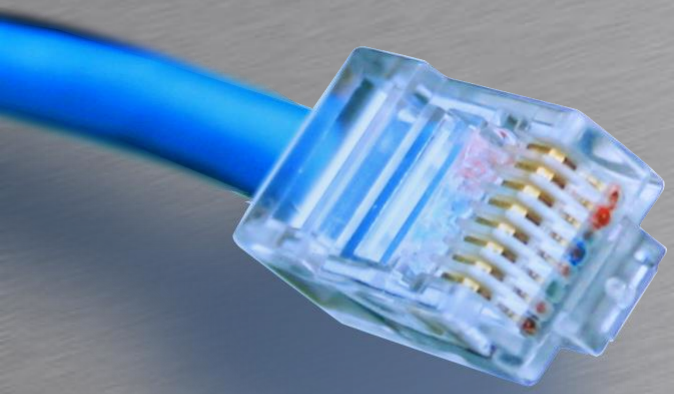
SRX

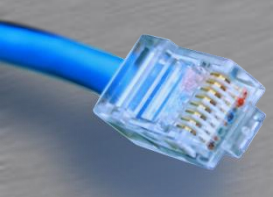


HOUSE OF TECHNOLOGY

– en del af mercantec

SRX Firewalls

Rasmus Elmholt V1.0



Deployment

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Branch SRX Series
  - SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650
  - Fokus for dette kursus
- Data Center SRX Series
  - SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

Branch SRX

HOUSE OF TECHNOLOGY
– en del af mercantec+

- SRX100
  - Eight 10/100 Ethernet LAN ports and 1 USB port (support for 3G USB)

SRX100	Performance
Firewall performance	700Mbps
IPS Performance	75Mbps
VPN Performance	65Mbps
Maximum concurrent sessions	32.000
New sessions/second	1.800
Maximum security policies	384

Branch SRX

HOUSE OF TECHNOLOGY
– en del af mercantec+

- SRX110
  - VDSL/ADSL2+ and Ethernet WAN interfaces
  - Eight 10/100 Ethernet LAN ports and two USB port (support for 3G USB)

SRX110	Performance
Firewall performance	700Mbps
IPS Performance	75Mbps
VPN Performance	65Mbps
Maximum concurrent sessions	32.000
New sessions/second	1.800
Maximum security policies	384

Branch SRX

- SRX210
  - Two 10/100/1000 Ethernet and 6 10/100 Ethernet LAN ports, 1 Mini-PIM slot, and 2 USB ports (support for 3G USB)
  - Factory option of 4 dynamic Power over Ethernet (PoE) ports 802.3af
  - Support for T1/E1, serial, ADSL/2/2+, VDSL, G.SHDSL, and Ethernet small form-factor pluggable transceiver (SFP)

SRX210	Performance
Firewall performance	850Mbps
IPS Performance	65Mbps
VPN Performance	85Mbps
Maximum concurrent sessions	64.000
New sessions/second	2.200
Maximum security policies	512

Branch SRX

HOUSE OF TECHNOLOGY
– en del af mercantec+

- SRX220
  - Eight 10/100/1000 Ethernet LAN ports, 2 Mini-PIM slots
  - Factory option of 8 PoE ports; PoE+ 802.3at, backwards compatible with 802.3af
  - Support for T1/E1, serial, ADSL/2/2+, VDSL, G.SHDSL, and Ethernet SFP

SRX220	Performance
Firewall performance	950Mbps
IPS Performance	80Mbps
VPN Performance	100Mbps
Maximum concurrent sessions	96.000
New sessions/second	2.800
Maximum security policies	2.048

Branch SRX

HOUSE OF TECHNOLOGY
– en del af mercantec+

- SRX240
  - 16 10/100/1000 Ethernet LAN ports, 4 Mini-PIM slots
  - Factory option of 16 PoE ports; PoE+ 802.3at, backwards compatible with 802.3af
  - Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, and Ethernet SFP

SRX240	Performance
Firewall performance	1.8Gbps
IPS Performance	230Mbps
VPN Performance	300Mbps
Maximum concurrent sessions	256.000
New sessions/second	8.500
Maximum security policies	4.096

Branch SRX

- SRX550
  - Ten fixed Ethernet ports (6 10/100/1000 Copper, 4 SFP), 2 Mini-PIM slots, 6 GPIM slots or multiple GPIM and XPIM combinations
  - Support for T1/E1, serial, ADSL2/2+, VDSL, G.SHDSL, DS3/E3, Gigabit Ethernet ports; supports up to 52 Ethernet
  - ports including SFP; 40 switch ports with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af
  - (or 50 non-PoE 10/100/1000 Copper ports), 10GbE

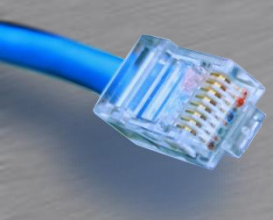
SRX550	Performance
Firewall performance	5.5Gbps
IPS Performance	800Mbps
VPN Performance	1.0Gbps
Maximum concurrent sessions	375.000
New sessions/second	27.000
Maximum security policies	7.256

Branch SRX

HOUSE OF TECHNOLOGY
– en del af mercantec+

- SRX650
  - Four fixed ports 10/100/1000 Ethernet LAN ports, 8 GPIM slots or multiple GPIM and XPIM combinations
  - Support for T1, E1, DS3/E3, Ethernet ports; supports up to 52 Ethernet ports including SFP; 48 switch ports with optional PoE including 802.3at, PoE+, backwards compatible with 802.3af (or 52 non-PoE 10/100/1000 Copperports), 10GbE

SRX650	Perfo
Firewall performance	7Gbps
IPS Performance	3Gbps
VPN Performance	1.5Gbps
Maximum concurrent sessions	512.000
New sessions/second	35.000
Maximum security policies	8.192



Packet modes

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Alle branch SRX enheder arbejder i Flow-based forwarding
  - Et flow valideres og retur trafik tillades
  - Trafik skal tillades
  - Gælder også til Routing Engine
- Juniper Routere kører Packet-based forwarding
  - Hver pakke valideres for sig.
  - Alt er tilladt med mindre det blokeres.

Packet modes

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Konfiguration
  - Konfigureres under security forwarding-options stanza

```
set security forwarding-options family mpls mode packet-based
set security forwarding-options family iso mode packet-based
set security forwarding-options family inet6 mode packet-based
```

  - Kan også konfigureres pr. firewall filter(Eksempel mangler)

- Default Flow based

```
user1@SRX07> show security flow status
  Flow forwarding mode:
    Inet forwarding mode: flow based
    Inet6 forwarding mode: drop
    MPLS forwarding mode: drop
    ISO forwarding mode: drop
  Flow trace status
    Flow tracing status: off
  Flow session distribution
    Distribution mode: RR-based
```

Zoner

- SRX enheder arbejder med zoner
  - Security Zones
    - Bruges til at adskille interfaces i forskellige sikkerheds zoner
    - Flere porte kan være i samme zone

```
[edit security zones]
user1@SRX07# show
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        vlan.0;
    }
}
```

  - Functional Zones
    - Bruges til management zoner(Bliver ikke dækket her)

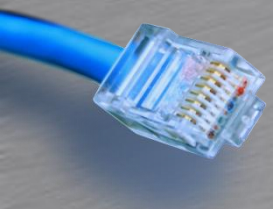
Zoner

HOUSE OF TECHNOLOGY

– en del af mercantec+

- SRX enheder arbejder med zoner
  - Host-inbound-traffic
    - Definerer trafik til kassen og ikke transit trafik.
    - Kan defineres på en zone eller på et interface
    - Nogle services kan kun ligge på et interface(DHCP)

```
[edit security zones]
user1@SRX07# show
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        vlan.0;
    }
}
```



Zoner

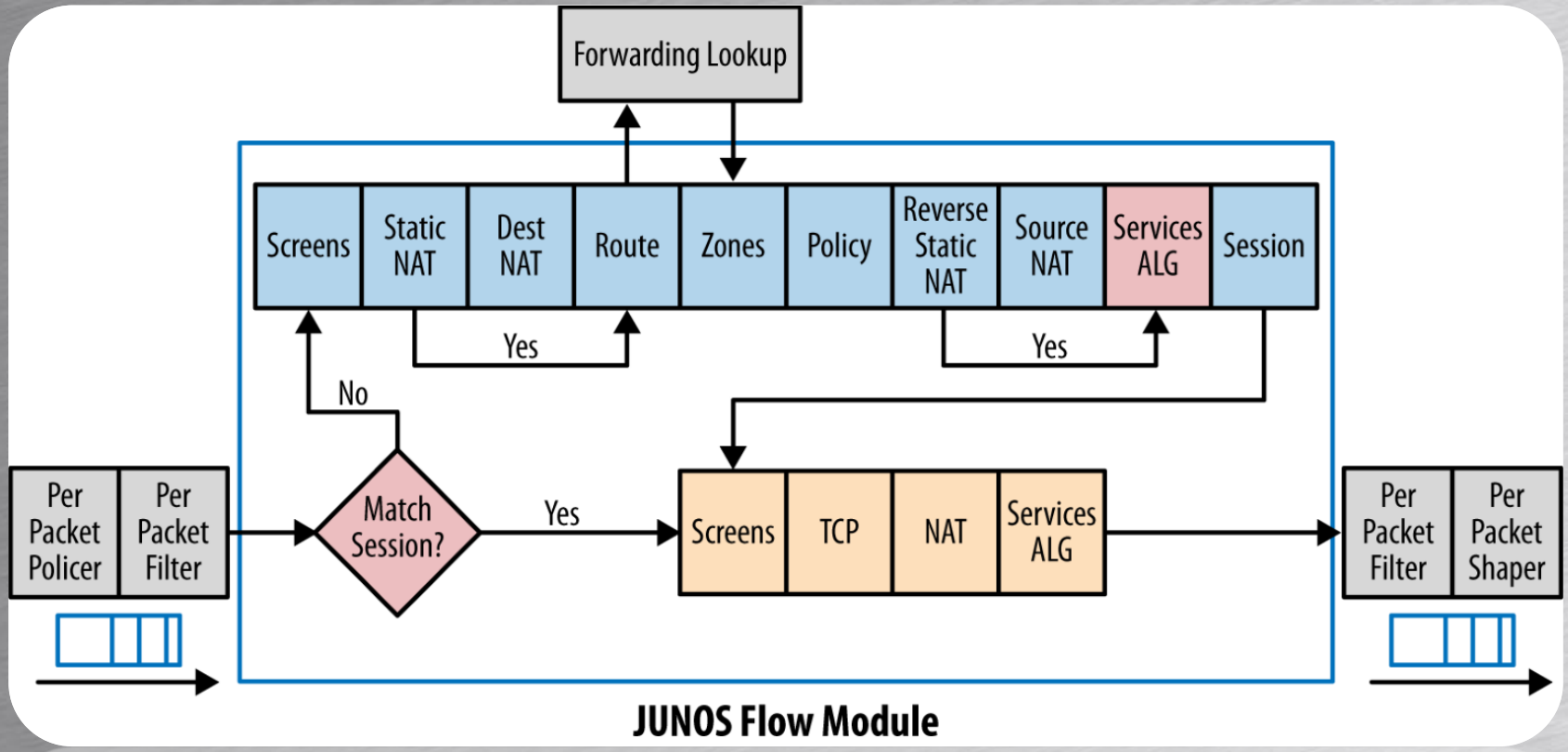
HOUSE OF TECHNOLOGY

– en del af mercantec

- Opgave!!

Packet Flow

- Pakker igennem en SRX
  - Alt lookup sker i HW/PFE



Security Policy

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Evaluering af pakker igennem sikkerheds politikker
  - Zoner
    - Fra og til zoner
  - Adresser
    - Source og destinations adresser
  - Application
    - Applications Objects
  - Actions
    - Pakker der matcher en politik skal behandles

Security Policy

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Evaluering af pakker igennem sikkerheds politikker
  - Fra top til bund.
  - Match afbryder
  - Implicit Deny

```
[edit security policies from-zone trust to-zone untrust]
user1@SRX07# show
policy trust-to-untrust-icmp {
    match {
        source-address any;
        destination-address any;
        application [ junos-icmp-all ];
    }
    then {
        drop;
        log {
            session-init;
        }
    }
```

```
policy trust-to-untrust-http {
    match {
        source-address any;
        destination-address any;
        application [ junos-http junos-https ];
    }
    then {
        permit;
    }
}
```

Security Policy

HOUSE OF TECHNOLOGY
– en del af mercantec

- Evaluering af pakker igennem sikkerheds politikker
  - Fra top til bund.
  - Match afbryder
  - Implicit Deny

```
user1@SRX07# set ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except   Don't inherit configuration data from these groups
> count                 Enable count
  deny                  Deny packets
> log                   Enable log
> permit                Permit packets
  reject                Reject packets
```

Security Policy

HOUSE OF TECHNOLOGY

– en del af mercantec

- Opgave

Address book

- Fra JunOS version 11.2 kan adresser defines globalt i security stanza'en
- Før skulle de defineres under hver zone
- Skal bruges hvis man vil matche på adresser

```
[edit security]
rael@SRX240# show
address-book {
    global {
        address JServer-10.0.255.10 {
            description "Server with web server and so on";
            10.0.255.10/32;
        }
        address SRX07-10.0.0.26 {
            description "SRX07 Firewall";
            10.0.0.26/32;
        }
    }
}
```

Address book

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Adresse objekter kan indeholde
  - IPv4 adresser
  - IPv6 adresser
  - Netværk/Prefixer
- Bruges af en policy

```
from-zone untrust to-zone trust {
        policy untrust-to-trust {
            match {
                source-address any;
                destination-address [ JServer-10.0.255.10 SRX07-10.0.0.26 ];
                application [ junos-http junos-ssh ];
            }
            then {
                permit;
            }
        }
    }
```

Address book

HOUSE OF TECHNOLOGY – en del af mercantec

- DNS adresse objekter
  - DNS Server skal være konfigureret
  - Kan indeholde op til 32 IP lookups
  - IPv4 & IPv6
  - Prefetcher men overholder DNS TTL

```
[edit security]
rael@SRX240# show address-book global
address www.bing.com {
    dns-name www.bing.com;
}
```

Address book

- Lav en opgave

Debug

HOUSE OF TECHNOLOGY

– en del af mercantec+

```
[edit security]
rael@SRX240# run show security policies hit-count
Logical system: root-logical-system
 Index   From zone        To zone          Name            Policy count
 1       trust            trust            trust-to-trust 12
 2       trust            untrust          trust-to-untrust 10767
 3       untrust          trust            untrust-to-trust 60

Number of policy: 3
```

```
rael@SRX240> show security flow session
Session ID: 19988, Policy name: untrust-to-trust/6, Timeout: 1422, Valid
  In: 192.168.146.103/58554 --> 192.168.146.100/2222;tcp, If: vlan.99, Pkts: 23, Bytes: 2970
  Out: 10.0.255.10/22 --> 192.168.146.103/58554;tcp, If: vlan.10, Pkts: 26, Bytes: 5585

Session ID: 20072, Policy name: trust-to-untrust/4, Timeout: 58, Valid
  In: 10.0.0.26/123 --> 83.90.47.30/123;udp, If: ge-0/0/7.0, Pkts: 1, Bytes: 76
  Out: 83.90.47.30/123 --> 192.168.146.100/4763;udp, If: vlan.99, Pkts: 1, Bytes: 76
```

Debug

HOUSE OF TECHNOLOGY

– en del af mercantec

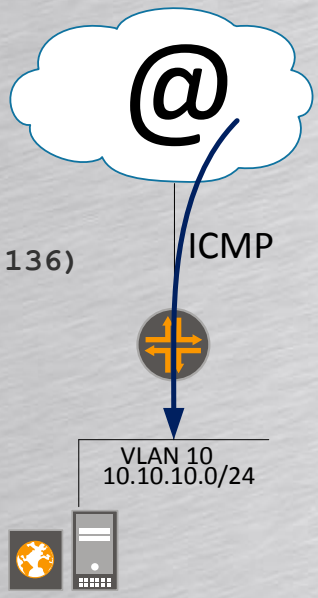
```
[edit security]
rael@SRX240# run show security policies hit-count
Logical system: root-logical-system
 Index   From zone        To zone          Name            Policy count
 1       trust            trust            trust-to-trust 12
 2       trust            untrust          trust-to-untrust 10767
 3       untrust          trust            untrust-to-trust 60

Number of policy: 3
```

Debug

HOUSE OF TECHNOLOGY
– en del af mercantec

– Her pinges der fra ydersiden til et inderside netværk.

```
[edit]
root@SRX07# run show interfaces ge-0/0/0.0 extensive
  Logical interface ge-0/0/0.0 (Index 71) (SNMP ifIndex 510) (Generation 136)
    Flags: SNMP-Traps 0x0 Encapsulation: ENET2
Security: Zone: untrust
    Allowed host-inbound traffic : dhcp tftp
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    171
      ICMP packets :                    21656
Flow error statistics (Packets dropped due to):
      No zone or NULL zone binding      0
      Policy denied:                    3
      Security association not active:  0
Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.0.0.24/30, Local: 10.0.0.26, Broadcast: 10.0.0.27,
        Generation: 146
```



Debug

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Opret en logfil med match på flows

```
[edit]
root@SRX07# show system syslog file traffic-log
any any;
match RT_FLOW_SESSION;
```

- Konfigurer logging på policy
  - Session-close når man tillader trafik, da den giver mere info
  - Session-init når man blokerer trafik eller lange sessioner

```
[edit security policies]
root@SRX07# show | display set relative
set from-zone trust to-zone untrust policy trust-to-untrust match source-address any
set from-zone trust to-zone untrust policy trust-to-untrust match destination-address any
set from-zone trust to-zone untrust policy trust-to-untrust match application any
set from-zone trust to-zone untrust policy trust-to-untrust then permit
set from-zone trust to-zone untrust policy trust-to-untrust then log session-close
```