NAT

HOUSE OF TECHNOLOGY

– en del af mercantec⁺

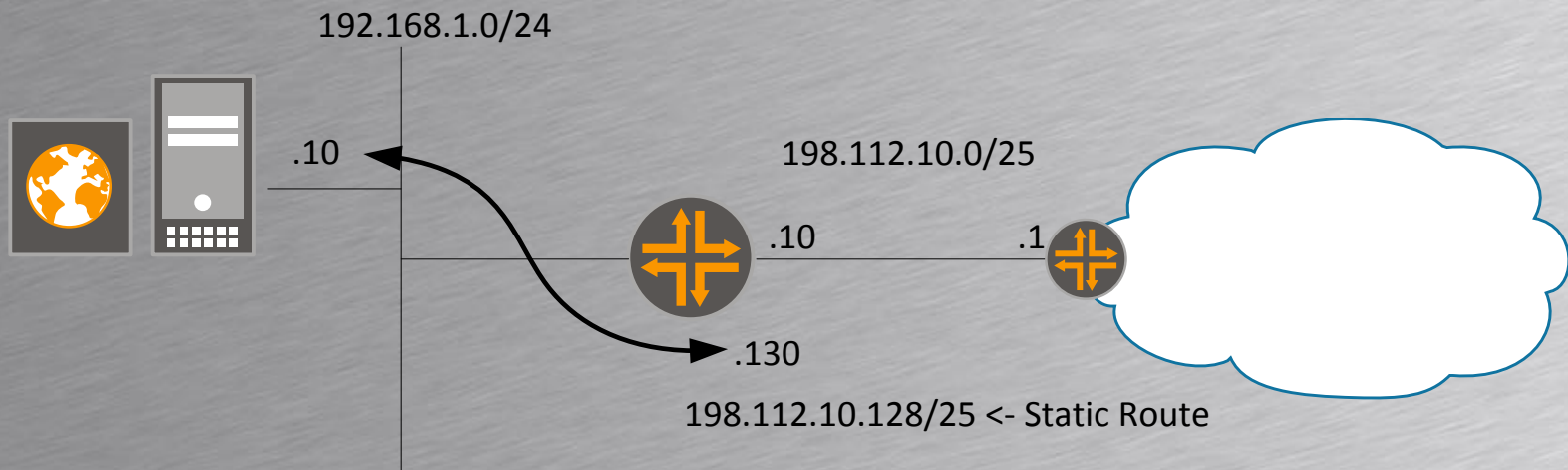## Typer og konfiguration

Rasmus Elmholt V1.0

- På SRX kasserne arbejder vi med 3 typer nat
  - Static
    - One-to-one
  - Destination
    - One-to-many
  - Source
    - Many-to-many
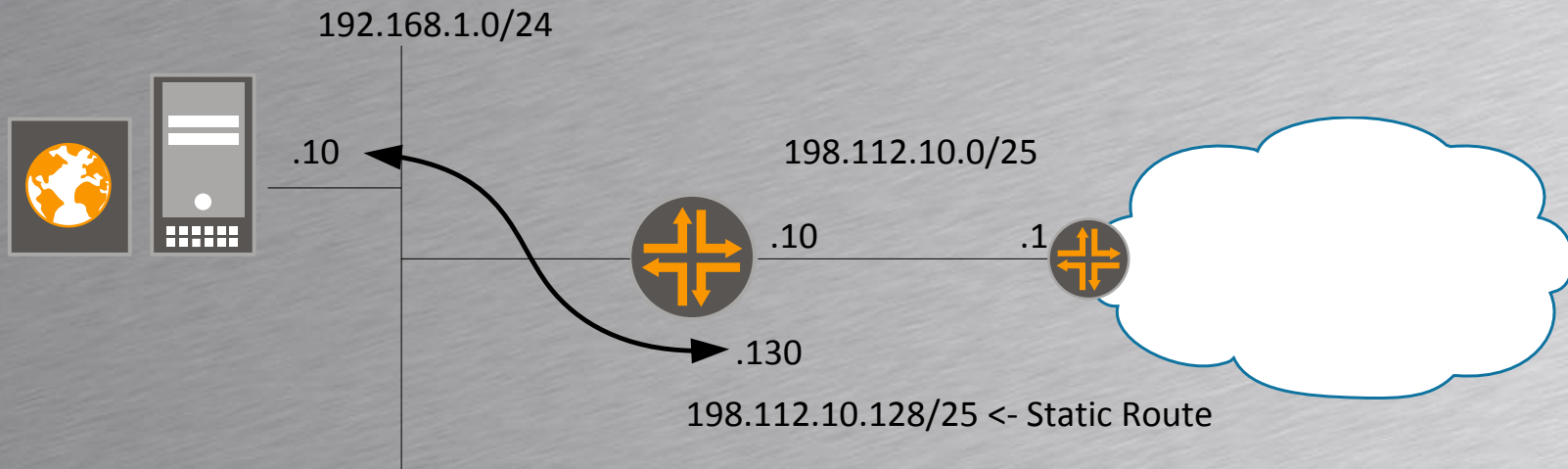
Static

- Oversætter en adresse til en anden
- Virker 2 vejs
  - Intern til ekstern
  - Ekstern til intern

192.168.1.0/24

.10

198.112.10.0/25

.10

.1

.130

198.112.10.128/25 <- Static Route

Inside Local	Outside Local	Inside Gobal	Outside Global
192.168.1.10	*	198.112.10.130	*

Static

192.168.1.0/24

.10

198.112.10.0/25

.10   .1

.130

198.112.10.128/25 <- Static Route

```
[edit security nat]
root@SRX07# show static
rule-set NAT-TO-SERVER {
    from zone untrust;
    rule TO-INTERNAL-SERVER {
        match {
            destination-address 198.112.10.130/32;
        }
        then {
            static-nat {
                prefix {
                    192.168.1.10/32;
                }
            }
        }
    }
}
```
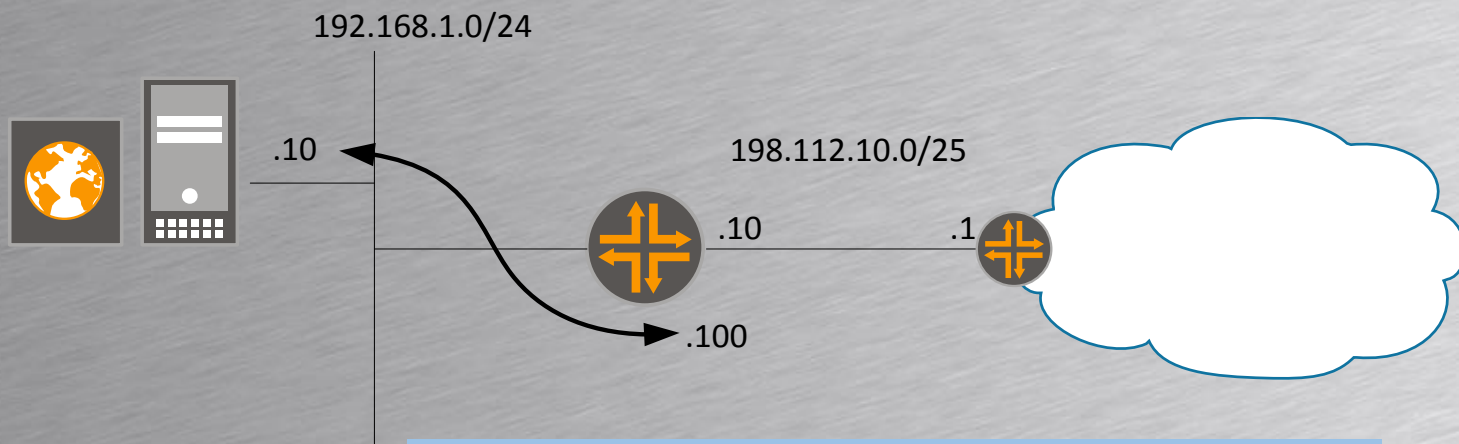
Zone eller interface

Yderside adresse

Inderside host

Static

- Statisk nat med Proxy ARP
  - Samme NAT konfiguration som før

192.168.1.0/24

.10

198.112.10.0/25

.10   .1

.100

Inside Local	Outside Local	Inside Gobal	Outside Global
192.168.1.10	*	198.112.10.100	*

```
proxy-arp {
    interface ge-0/0/0.20 {
        address {
            198.112.10.100/32;
        }
    }
}
```

Source

- Oversætter adresser til en eller flere
  - En vejs(retur trafik tillades)
  - Many-to-many/many-to-one
    - Både NAT og PAT

192.168.1.0/24

198.112.10.0/25

.10

.11

.10

.1

.100-110

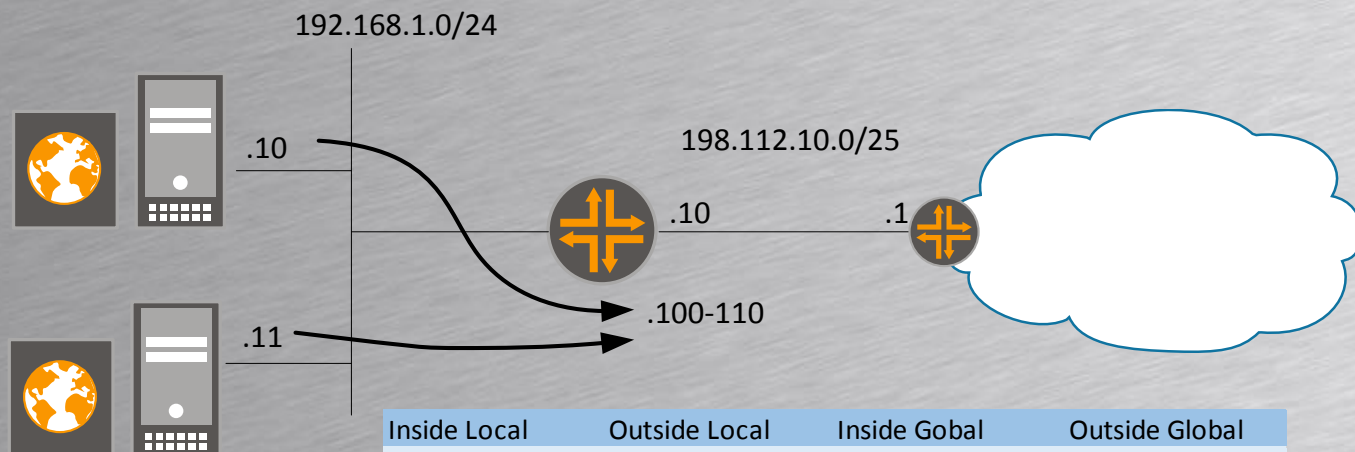| Inside Local	Outside Local	Inside Gobal	Outside Global
192.168.1.10	*	198.112.10.100	*
192.168.1.11	*	198.112.10.101	*
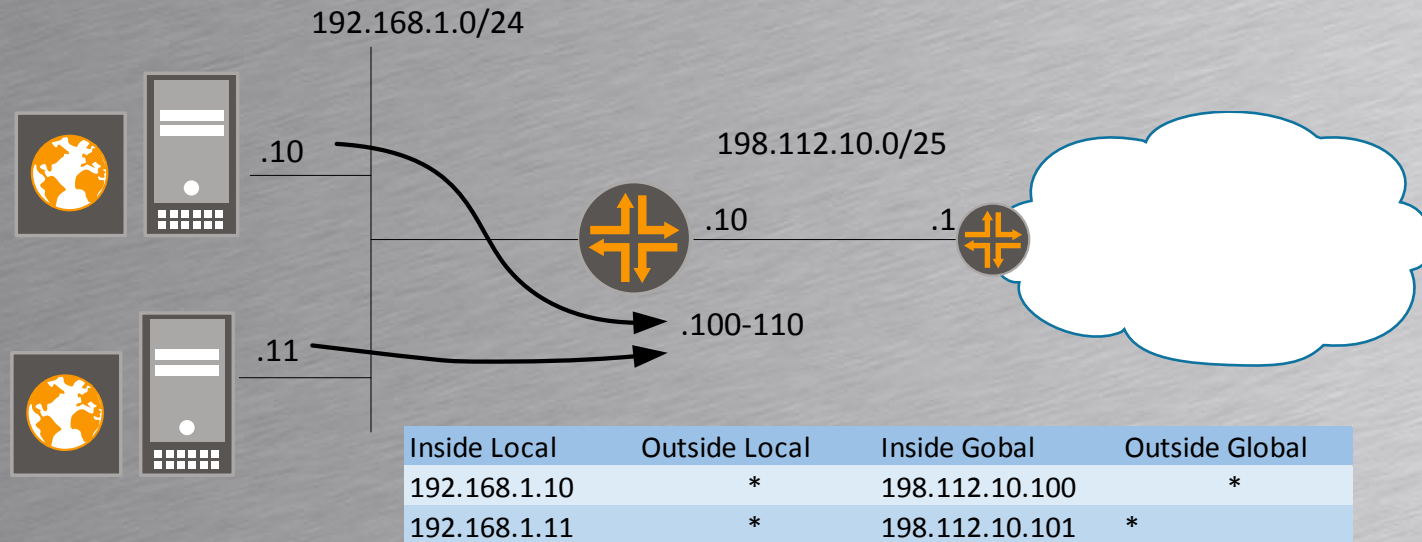
Source

```
pool NAT-POOL {
    address {
        198.112.10.100/32 to 198.112.10.110/32;
    }
    #port no-translation;
}
rule-set trust-to-untrust {
    from zone trust;
    to zone untrust;
    rule source-nat-rule {
        match {
            source-address 192.168.1.0/24;
        }
        then {
            source-nat pool NAT-POOL;
        }
    }
}
```
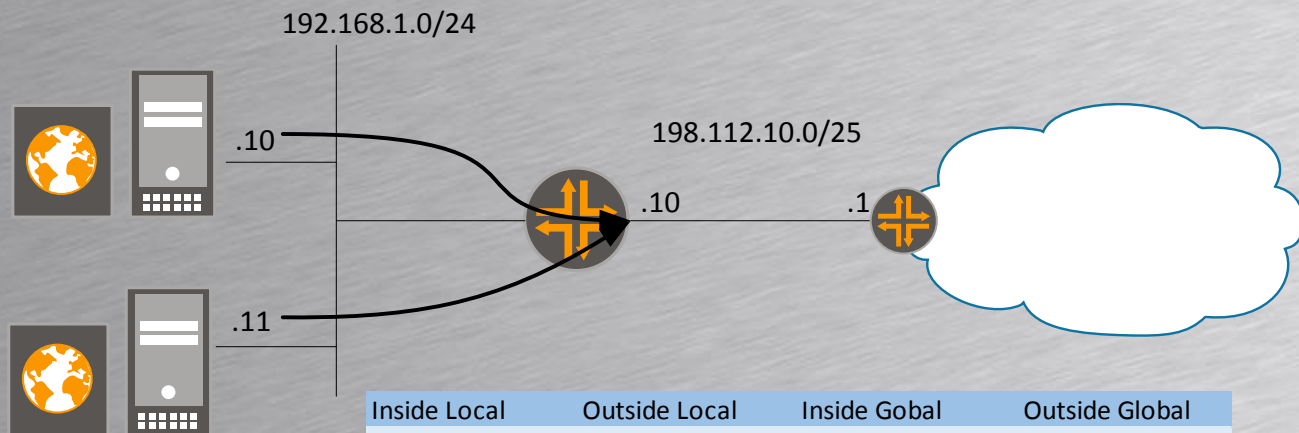
NAT i stedet for PAT

192.168.1.0/24

198.112.10.0/25

.10

.10   .1

.100-110

.11

Inside Local	Outside Local	Inside Gobal	Outside Global
192.168.1.10	*	198.112.10.100	*
192.168.1.11	*	198.112.10.101	*

```
rule-set trust-to-untrust {
    from zone trust;
    to zone untrust;
    rule source-nat-rule {
        match {
            source-address 192.168.1.0/24;
        }
        then {
            source-nat {
                interface;
            }

        }
    }
}
```
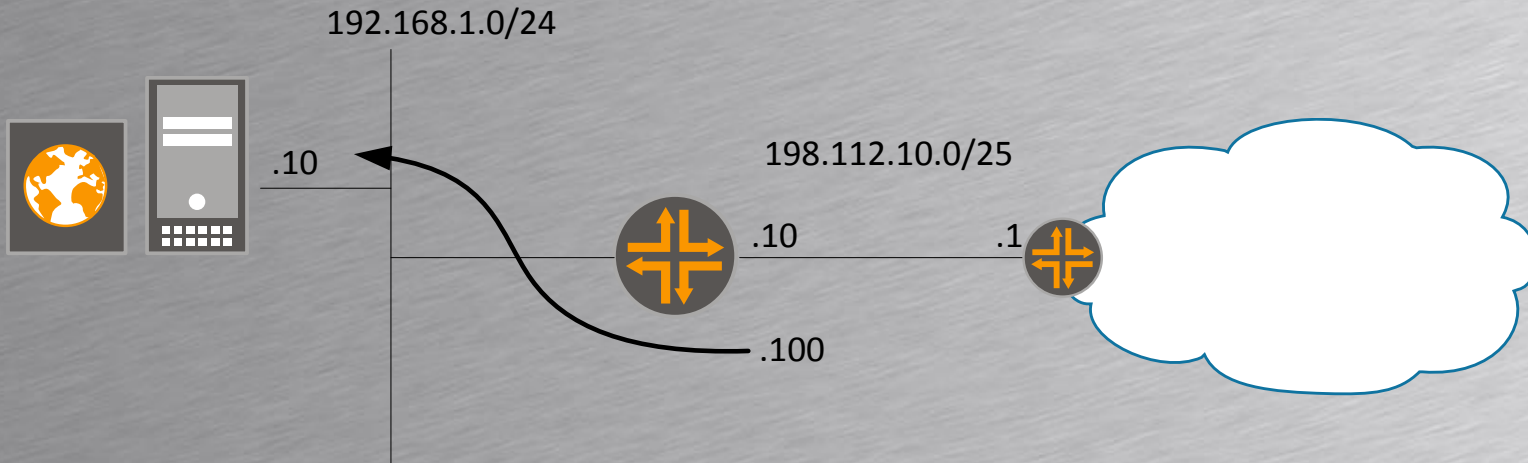
192.168.1.0/24

.10

198.112.10.0/25

.10   .1

.11

Inside Local	Outside Local	Inside Gobal	Outside Global
192.168.1.10	*	198.112.10.10	*
192.168.1.11	*	198.112.10.10	*

Destination

- Oversætter adresser til en eller flere
  - En vejs(retur trafik tillades)
  - one-to-one/one-to-many
  - NAT/PAT

192.168.1.0/24

.10

198.112.10.0/25

.10   .1

.100

Inside Local	Outside Local	Inside Gobal	Outside Global
192.168.1.10	*	198.112.10.100	*

192.168.1.0/24

.10

198.112.10.0/25

.10

.1

.100
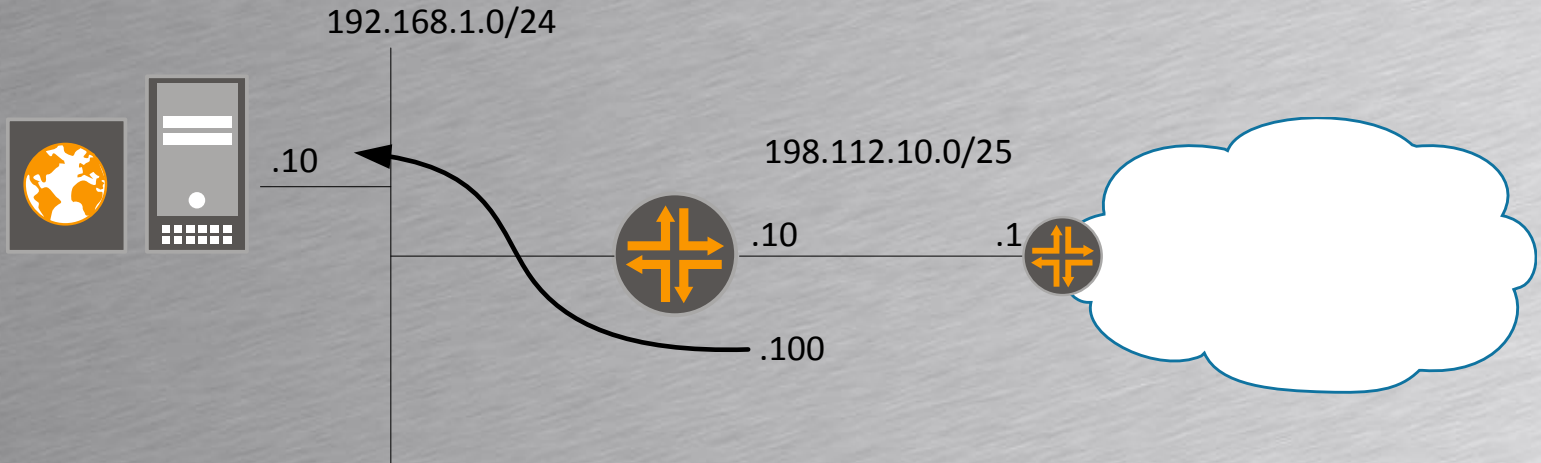
```
[edit security nat destination]
root@SRX07# show
pool WEB-SERVER {
    address 192.168.1.10/32 port 80;
}
rule-set DEST-NAT {
    from zone untrust;
    rule SINGLE-ADDRESS-NAT {
        match {
            destination-address 198.112.10.100/32;
            destination-port 80;
        }
        then {
            destination-nat pool WEB-SERVER;
        }
    }
}
```

Inside Local	Outside Local	Inside Gobal	Outside Global
192.168.1.10	*	198.112.10.100	*

```
proxy-arp {
    interface ge-0/0/0.20 {
        address {
            198.112.10.100/32;
        }
    }
}
```
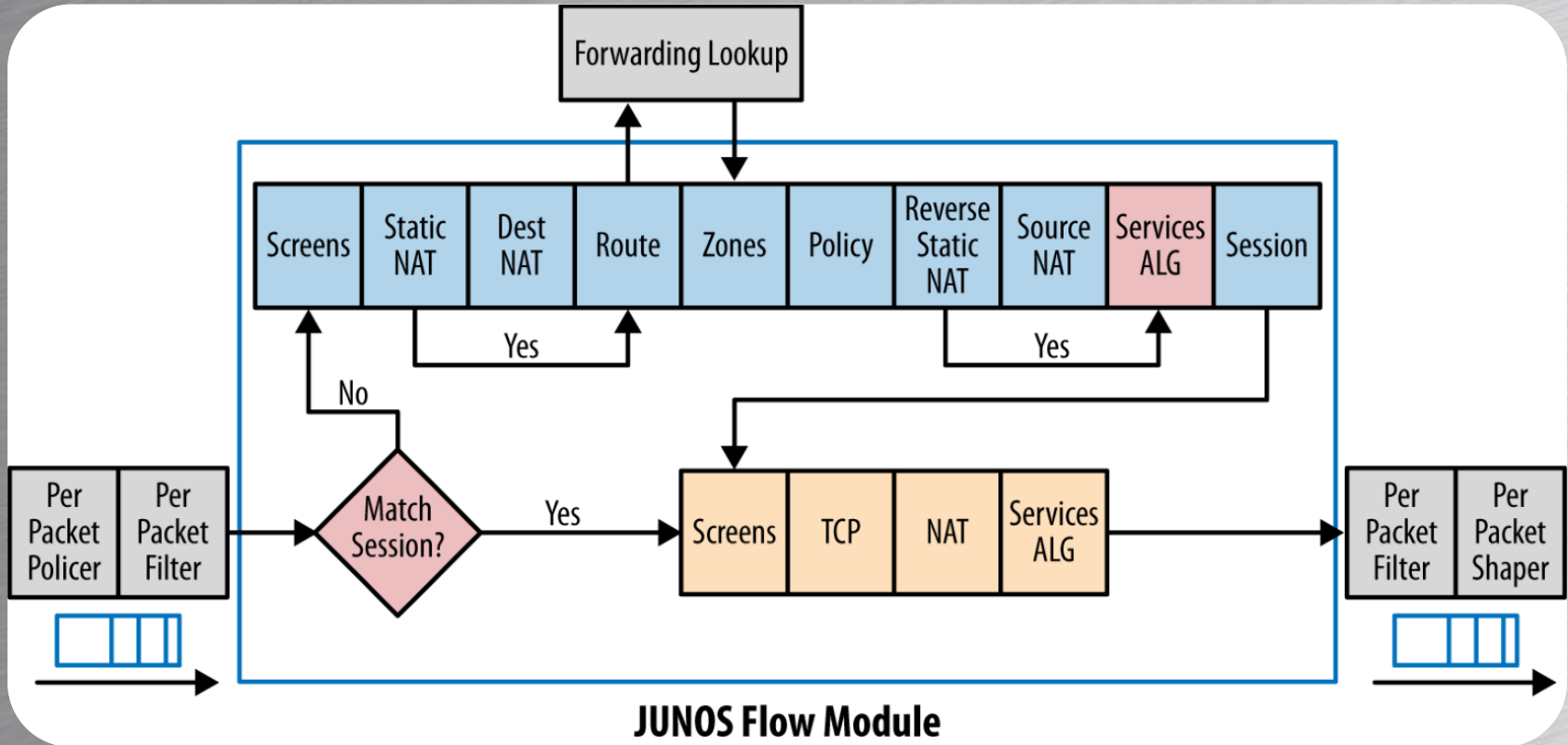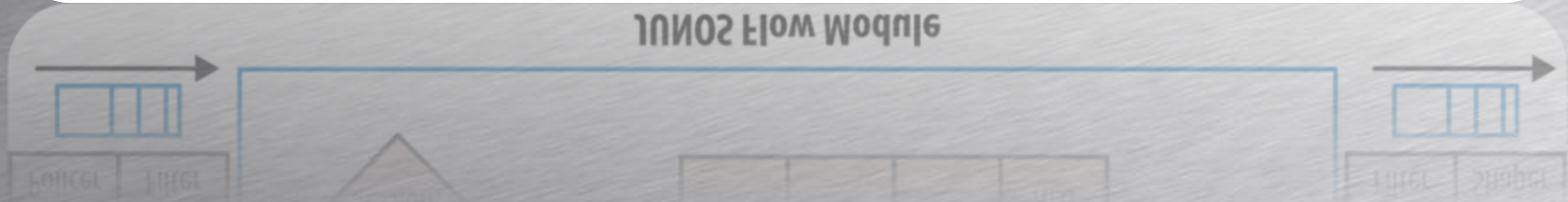
Flow

JUNOS Flow Module

- ## Kæd det sammen

```
[edit security nat destination]
root@SRX07# show
pool WEB-SERVER {
    address 192.168.1.10/32 port 80;
}
rule-set DEST-NAT {
    from zone untrust;
    rule SINGLE-ADDRESS-NAT {
        match {
            destination-address 198.112.10.100/32;
            destination-port 80;
        }
        then {
            destination-nat pool WEB-SERVER;
        }
    }
}
```