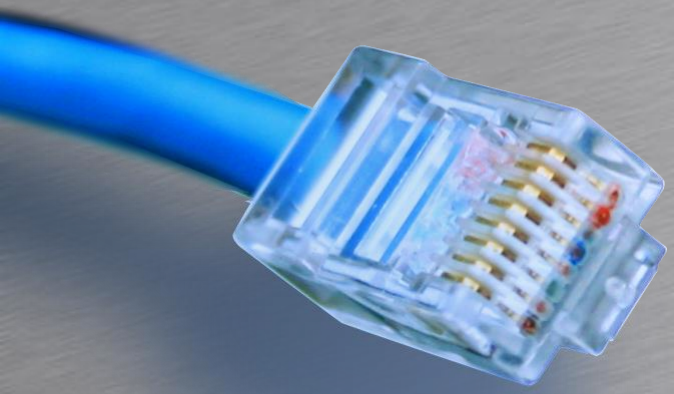
Cisco IOS



HOUSE OF TECHNOLOGY

– en del af mercantec+

ZONE BASED FIREWALL

Henrik Thomsen V1.0

Zone-based firewall

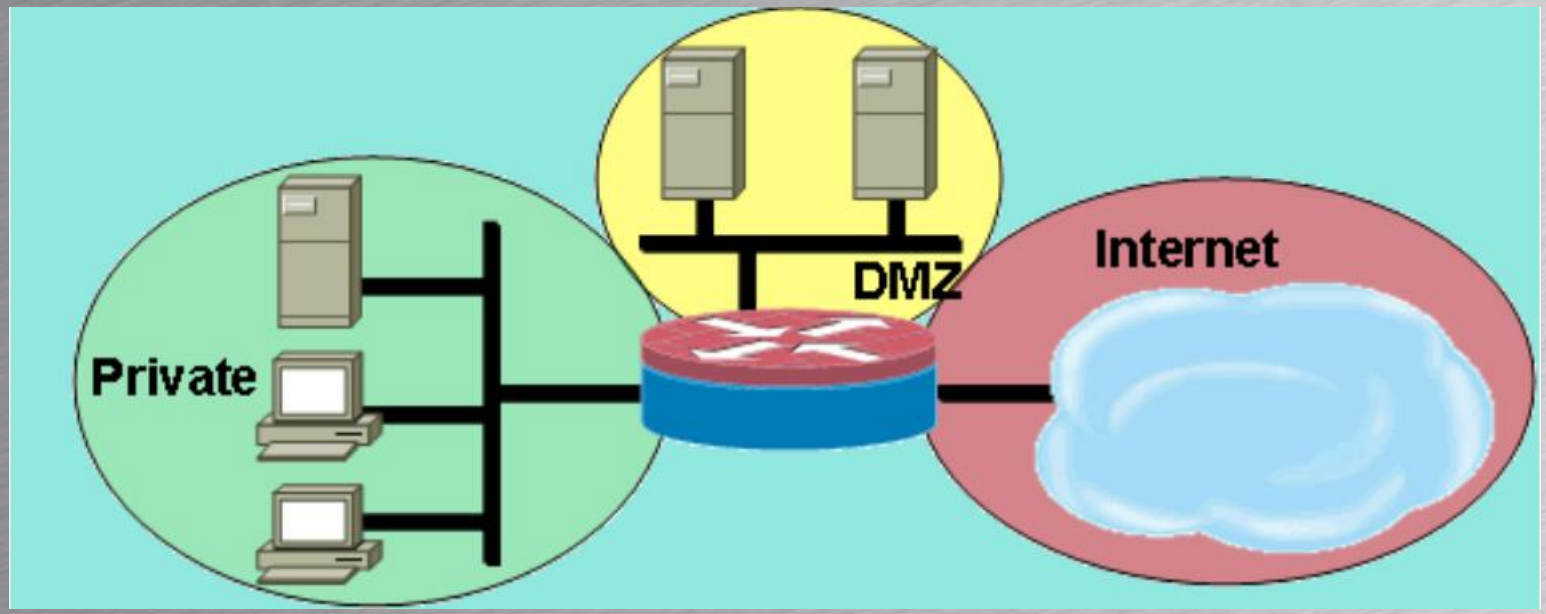
HOUSE OF TECHNOLOGY
– en del af mercantec

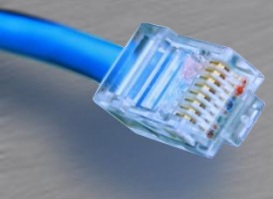
- ZFW
  - Zone-based Firewall eller Zone-based policy firewall
  - Fra IOS 12.4(9)T
- ZFW erstatter CBAC
  - Context-based Access Control
  - CBAC policies ofte forvirrende

Hvad er en Zone

HOUSE OF TECHNOLOGY
– en del af mercantec

- En zone definerer en grænse hvor trafik passerer til en anden region af netværket
  - I zonen inspiceres frafikken af en policy
  - Default policy er **deny all**





Hvad er en Zone

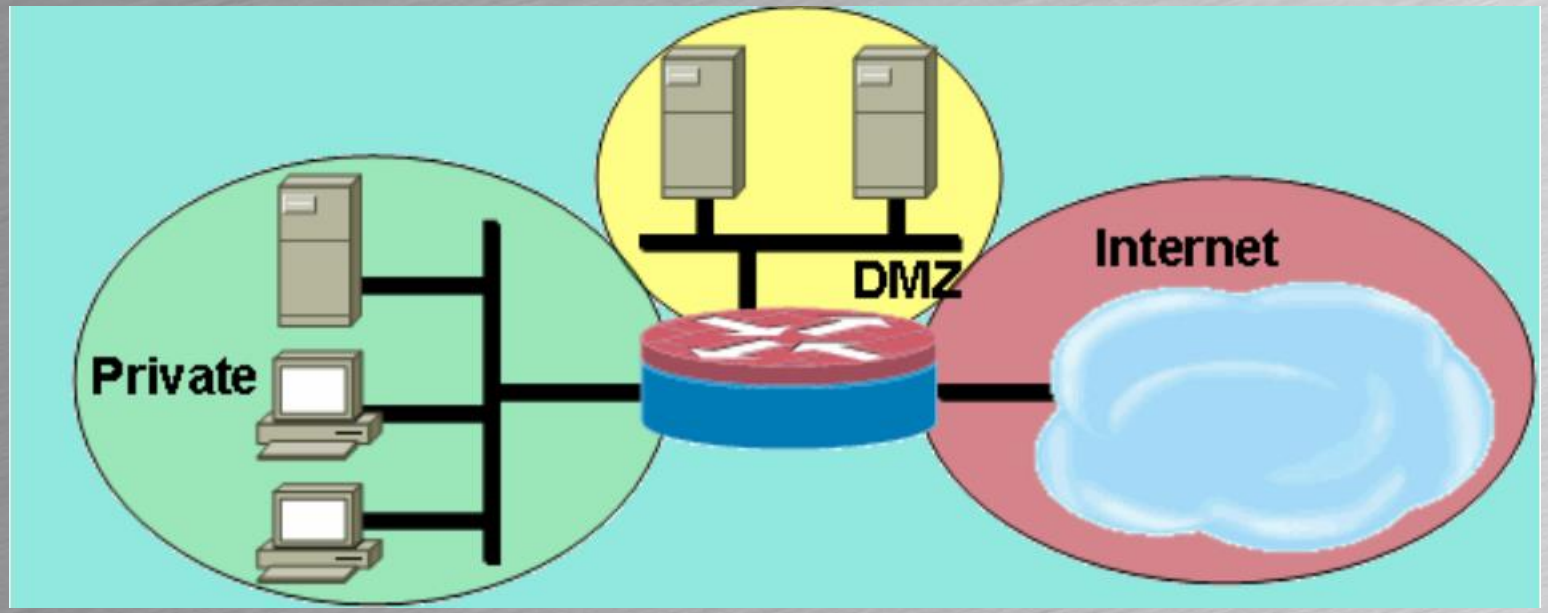
HOUSE OF TECHNOLOGY
– en del af mercantec+

- Konfigureres i CPL
  - Configuration Policy Language
  - Minder om Modular QoS CLI (MQC)
    - Anvendelse af class-maps i policy map.

```
class-map type inspect match-all ALL-PRIVATE
 match access-group 101
!
policy-map type inspect PRIV-PUB-PMAP
 class type inspect ALL-PRIVATE
  inspect
 class class-default
!
```

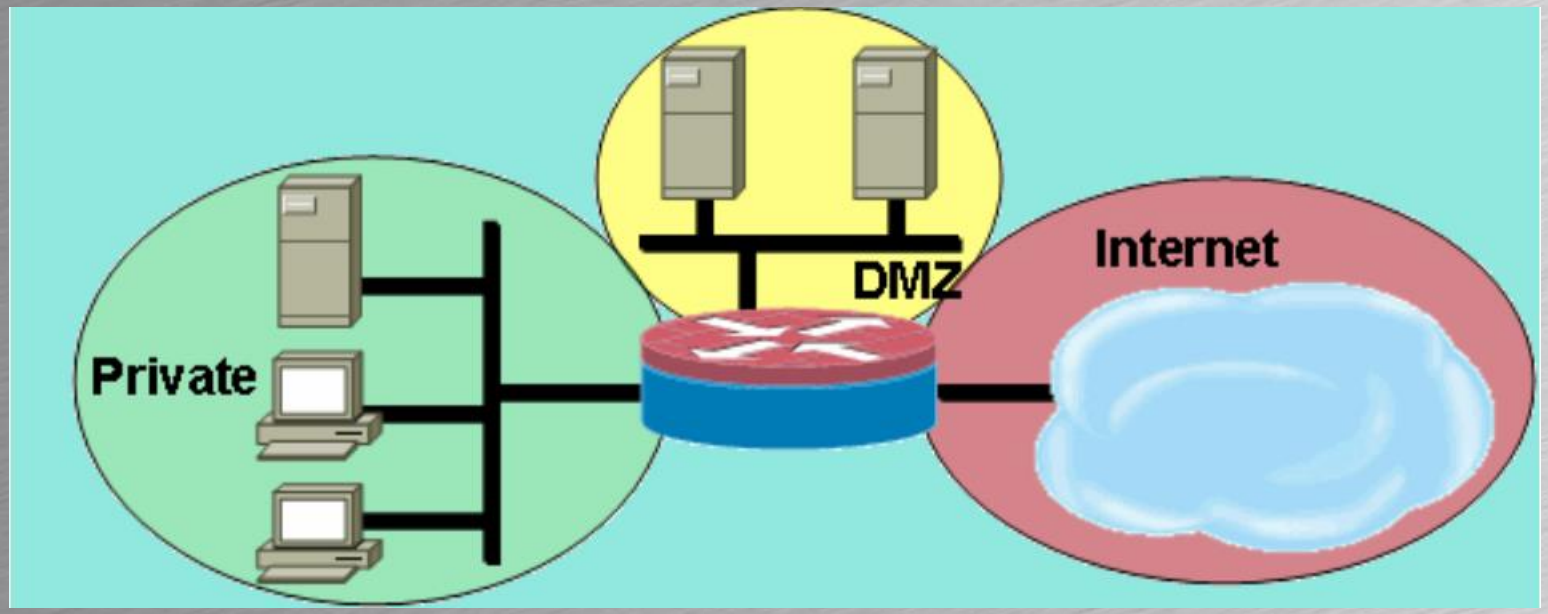
ZFW regler

- En zone skal konfigureres før et interface kan gøres medlem
- Et interface kan kun være i én zone
- Al trafik er default blokeret ud af zonen
  - Default - **Deny all**



ZFW regler

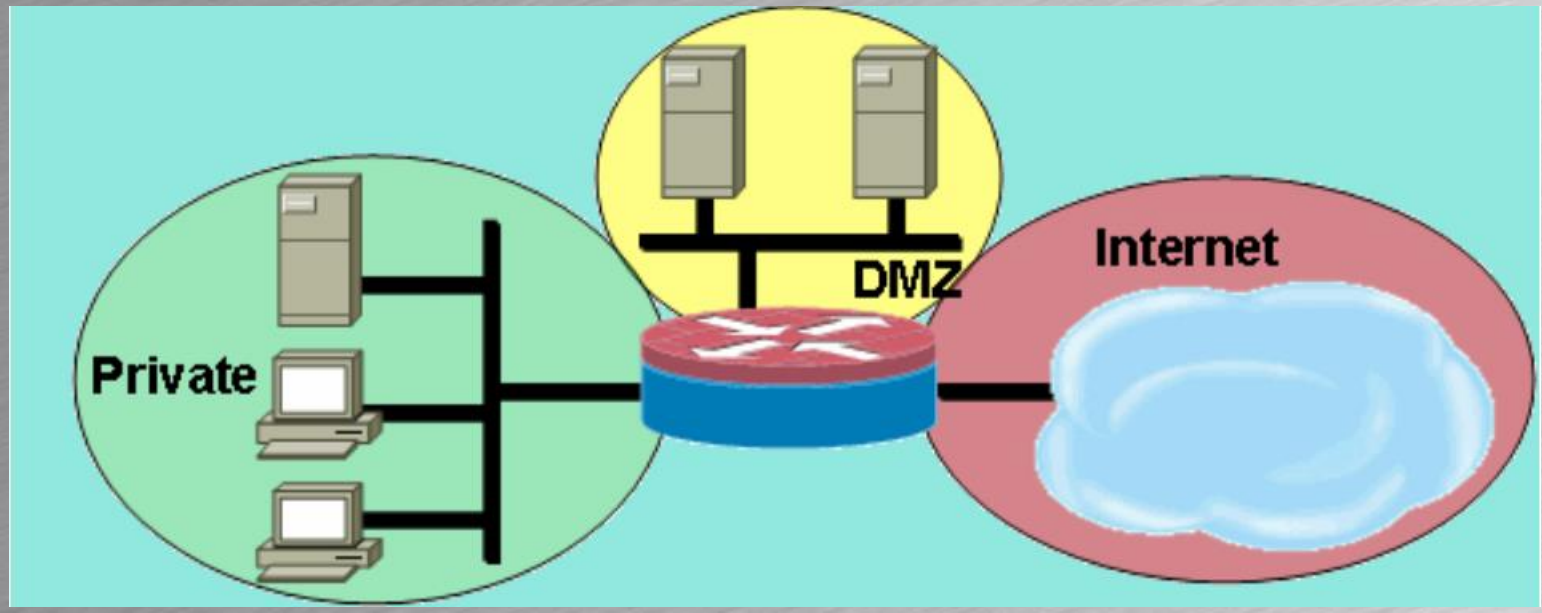
- Trafik mellem interfaces i samme zone tilladt
- Policies tillader trafik mellem zoner
- Ingen trafik fra interface i zone til interface der ikke er i en zone



ZFW eksempel

HOUSE OF TECHNOLOGY
– en del af mercantec+

- Tre zoner: Private, DMZ og internet
- Tre hoved policies
  - Private til DMZ zone
  - Private til Internet zone
  - Internet til DMZ zone



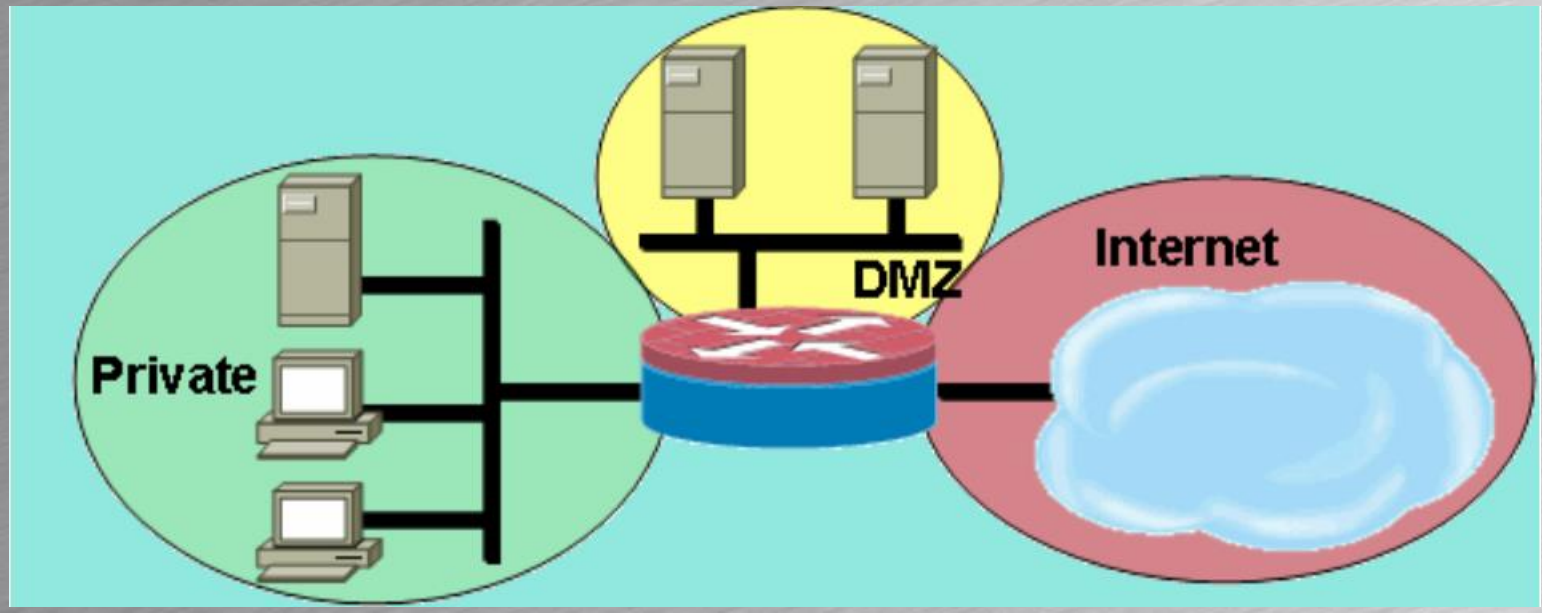
ZFW fremgangsmåde

HOUSE OF TECHNOLOGY – en del af mercantec

1. Definer zoner
2. Definer zone-par
3. Definer class-maps
    1. Beskriver trafikken som må passere mellem zoner
4. Definer policy-maps
    1. Beskriv hvad der skal ske med class-map trafikken
5. Tildel policy-maps til zone-par
6. Sæt interfaces i zonerne

1: Definer zoner

```
zone security PRIVATE
zone security DMZ
zone security INTERNET
```

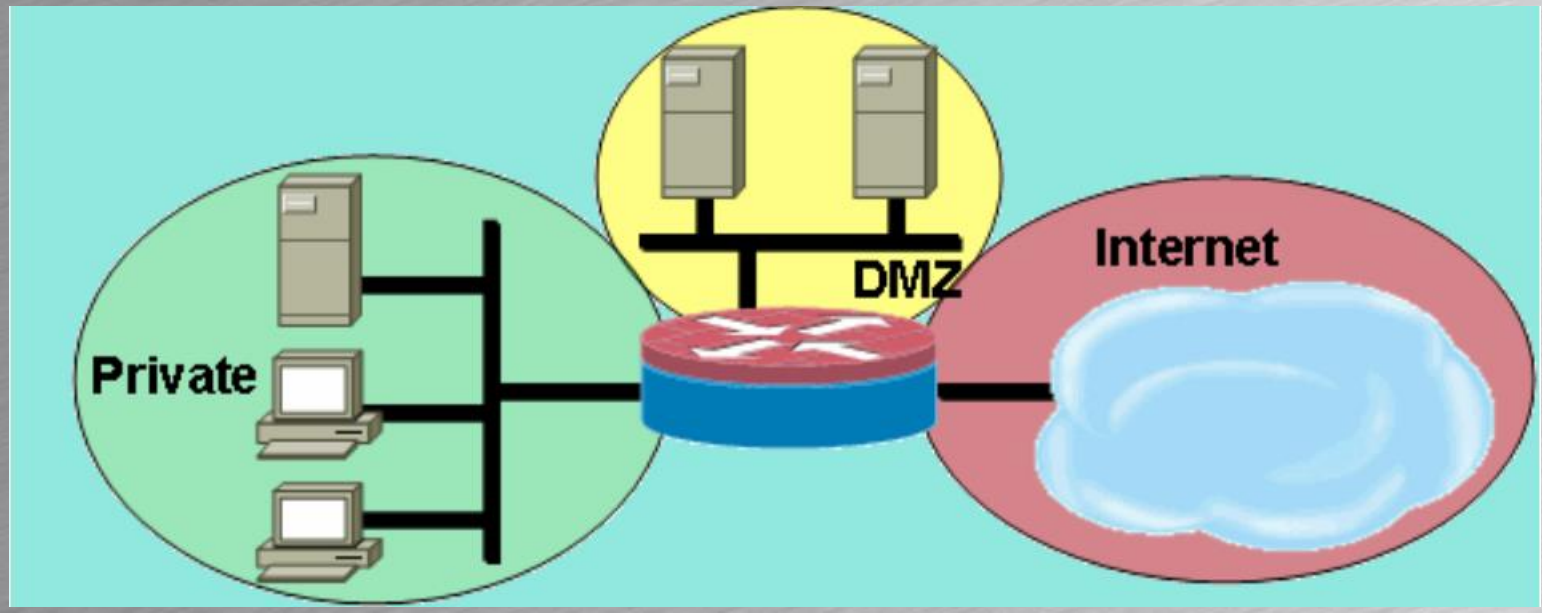


2: Definer zone-par

HOUSE OF TECHNOLOGY
– en del af mercantec+

```
zone-pair security PRI2DMZ source PRIVATE destination DMZ
zone-pair security PRI2INT source PRIVATE destination INTERNET
zone-pair security INT2DMZ source INTERNET destination DMZ
```

- Behøves ikke defineres på routeren nu
  - Men retninger af policies er vigtige at kende

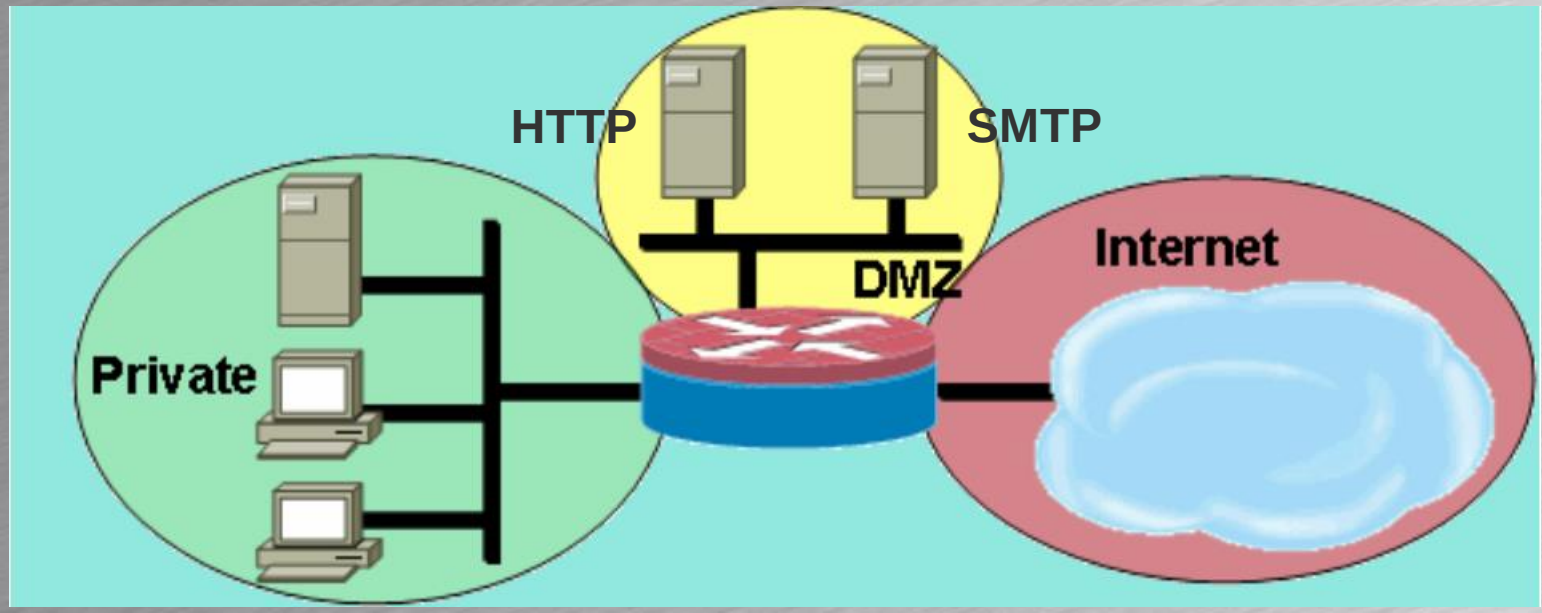


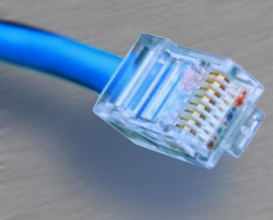
3B: Definer class-maps

HOUSE OF TECHNOLOGY
– en del af mercantec

```
class-map type inspect match-any INT2DMZ-CM
 match protocol http
 match protocol smtp
```

- Ulemper
  - HTTP trafik til alle IP i DMZ
  - SMTP trafik til alle IP i DMZ





3C: Definer class-maps

HOUSE OF TECHNOLOGY

– en del af mercantec

```
access-list 110 permit tcp any host 10.1.1.3 eq smtp
access-list 120 permit tcp any host 10.1.1.2 eq www
!
class-map type inspect match-all DMZ-HTTP-CM
 match access-group 120
 match protocol http
!
class-map type inspect match-all DMZ-SMTP-CM
 match access-group 110
 match protocol smtp
!
class-map type inspect match-any INT2DMZ-CM
 match class-map DMZ-HTTP-CM
 match class-map DMZ-SMTP-CM
```

- Mere sikker men uoverskuelig konstruktion

4: Definer policy-maps

HOUSE OF TECHNOLOGY

– en del af mercantec+

- Policy-maps definerer hvad der skal ske
- Trafik der matcher INT2DMZ-CM får lov at passere og retur trafik får lov at passere
- Alt andet trafik rammer **class-default** som dropper al trafik

```
class-map type inspect match-any INT2DMZ-CM
 match protocol http
 match protocol smtp
!
policy-map type inspect INT2DMZ-PM
 class type inspect INT2DMZ-CM
  inspect
 class class-default
  drop
```

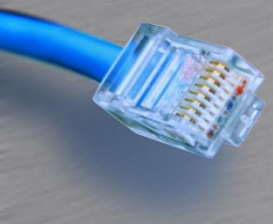
4: Definer policy-maps

HOUSE OF TECHNOLOGY – en del af mercantec+

- Tre mulige actions på policy-maps

DROP	Default action for al trafik. Trafikken droppes uden icmp unreachable til afsender. (Silent drop)
PASS	Trafikken får lov at passere, men kun i en retning. Returtrafik droppes
INSPECT	Trafikken får lov at passere og retur trafik får lov at passere. Routeren vedligeholder table over åbne TCP og UDP forbindelser

```
policy-map type inspect INT2DMZ-PM
 class type inspect INT2DMZ-CM
  inspect
 class class-default
  drop
```



5: policy-maps til zone-par

HOUSE OF TECHNOLOGY

– en del af mercantec

```
class-map type inspect match-any INT2DMZ-CM
 match protocol http
 match protocol smtp
!
policy-map type inspect INT2DMZ-PM
 class type inspect INT2DMZ-CM
  inspect
 class class-default
  drop
!
zone-pair security INT2DMZ source INTERNET destination DMZ
 service-policy type inspect INT2DMZ-PM
```

6: Sæt interfaces i zonerne

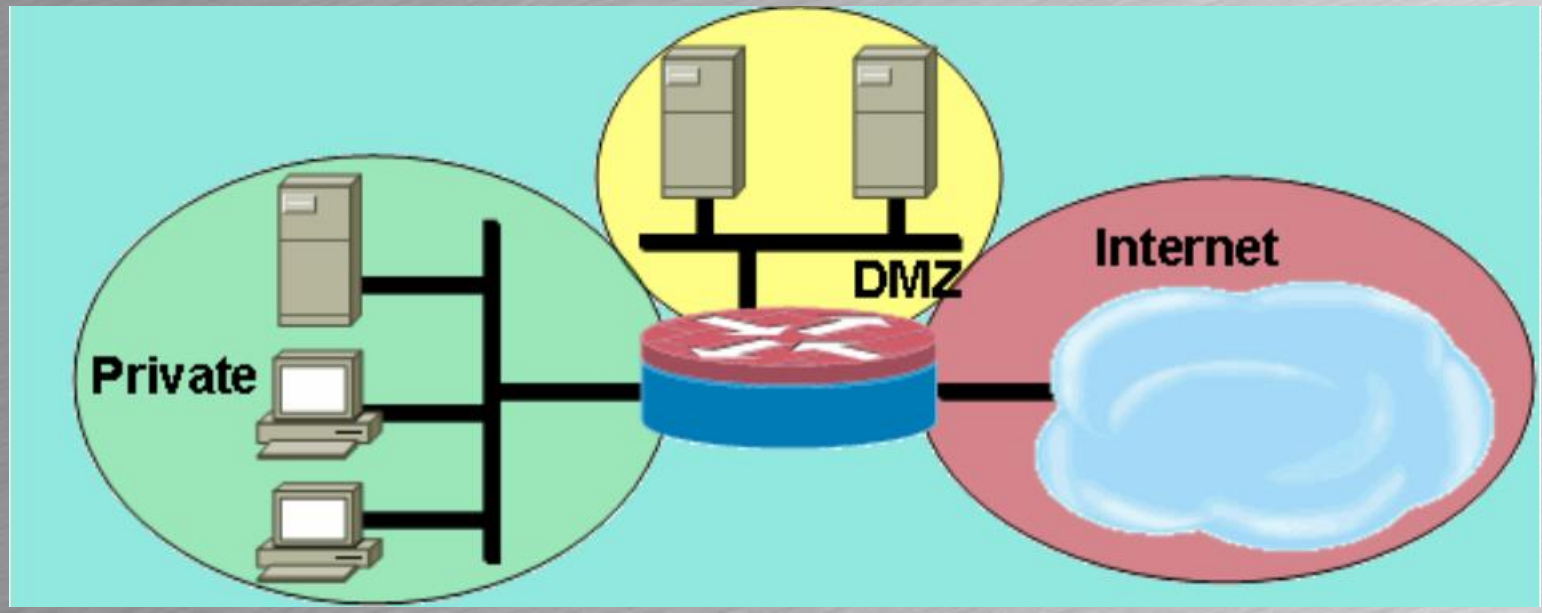
HOUSE OF TECHNOLOGY

– en del af mercantec

```
class-map type inspect match-any INT2DMZ-CM
 match protocol http
 match protocol smtp
!
policy-map type inspect INT2DMZ-PM
 class type inspect INT2DMZ-CM
  inspect
 class class-default
  drop
!
zone-pair security INT2DMZ source INTERNET destination DMZ
 service-policy type inspect INT2DMZ-PM
!
interface FastEthernet 0/1
 description Forbindelse til DMZ zone
 zone-member security DMZ
!
Interface FastEthernet 0/2
 description Forbindelse til ISP
 zone-member security INTERNET
```

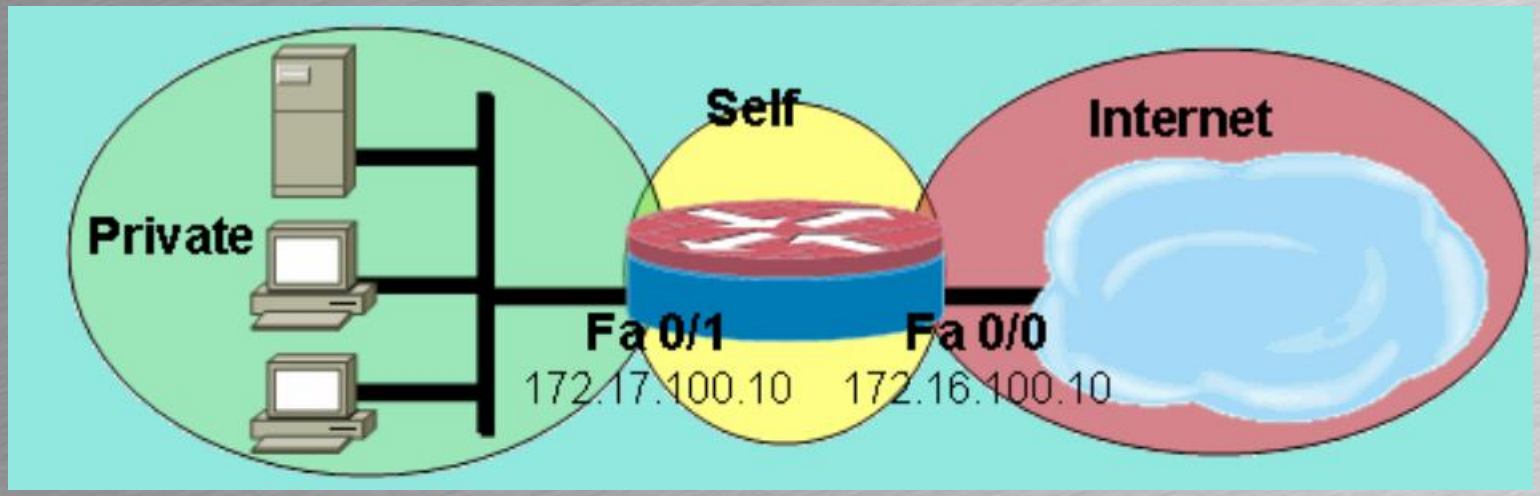
Indtil nu

- Regler for trafik fra zone PRI til DMZ lavet
- Mangler
  - PRI til INT og evt DMZ til PRI



ZFW regler – Self zone

- Trafik fra zone til self-zone tilladt
- Interfaces konfigureret i en zone
  - Trafik til IP adresser på interface i zoner er tilladt
    - De er alle i self-zone hvor trafik er **permit all**
    - Separate policies kan anvendes i self-zone



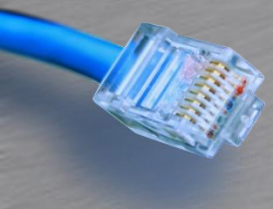
Eksempel: self zone

HOUSE OF TECHNOLOGY

– en del af mercantec+

```
class-map type inspect match-any INT2SELF-CM
 match access-group name MGMT
 match access-group name INT-ALLOW
!
policy-map type inspect INT2SELF-PM
 class type inspect INT2SELF-CM
  inspect
 class class-default
  drop log
!
zone-pair security INT2SELF source INT destination self
 service-policy type inspect INT2SELF-PM

!
ip access-list extended MGMT
 permit ip 10.10.1.0 0.0.0.255 any
ip access-list extended INT-ALLOW
 permit icmp any any
 permit udp any any eq bootps
```



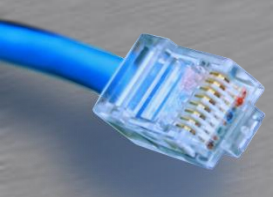
Show commands

HOUSE OF TECHNOLOGY

– en del af mercantec

```
Router#show zone security INT
Zone INT
  Description: this is test zone1
  Member Interfaces:
    FastEthernet0/0
```

```
Router#show zone-pair security
zone-pair name INT2DMZ
  Source-Zone INT Destination-Zone DMZ
  service-policy INT2DMZ-SP
```



Show

HOUSE OF TECHNOLOGY

– en del af mercantec+

```
Router#show policy-map type inspect zone-pair zp
Zone-pair: zp
 Service-policy : p1
  Class-map: c1 (match-all)
    Match: protocol tcp
    Inspect
     Session creations since subsystem startup or last reset 0
     Current (estab/half-open/terminating) [0:0:0]
     Maxever counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
     Last session creation rate 0
     Last half-open session total 0
  Class-map: class-default (match-any)
    Match: any
    Drop
      0 packets, 0 bytes
```