

HOUSE OF TECHNOLOGY  
- en del af mercantec\*



# Cisco ASA 5505

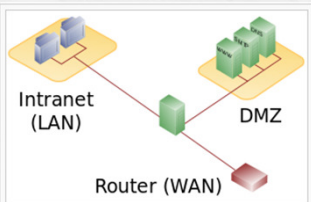
Vejledning

## Opsætning af DMZ-zone

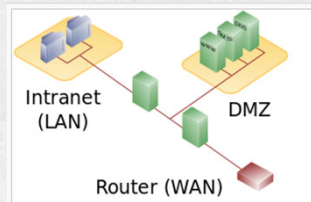
Hvad er en DMZ-zone???

HOUSE OF TECHNOLOGY  
- en del af mercantec\*

- En 'demilitariseret zone' eller 'ingen mands land'! 😊
  - [http://en.wikipedia.org/wiki/DMZ\\_%28computing%29](http://en.wikipedia.org/wiki/DMZ_%28computing%29)



3-legged network DMZ



Dual firewall DMZ

### Målet for vores ASA netværk

HOUSE OF TECHNOLOGY  
- en del af mercantec\*

The diagram illustrates a Cisco ASA5505 firewall configuration. The Internet (Outside) is connected to Port 0 (IP .93) and provides DHCP for the 192.168.63.0/24 network. The LAN (Inside) is connected to Port 1 (IP .1) and provides DHCP for the 192.168.1.0/24 network. The DMZ zone (DMZ) is connected to Port 2 (IP .1) and provides static IP addresses for the 10.0.0.0/24 network. A Test-Klient is connected to the Internet. A Webserver is connected to the DMZ zone. A DNS-server and Klient-Pc are connected to the LAN. A Switch connects the LAN and DMZ zones. A note indicates that DHCP is delivered to the Klient-Pc (DHCP delivered - check!).

- Et "standard" netværk med en trebenet firewall:
  - Internet (Outside)
  - LAN (Inside)
  - DMZ-zone (DMZ)
- Udgangspunkt:
  - Factory-reset!

### Bemærk!

HOUSE OF TECHNOLOGY  
- en del af mercantec\*

- ASA5505 er ingen almindelig Cisco router!
  - Den kører med sit eget og helt specielle software.
  - Man kan som udgangspunkt IKKE pinge igennem en ASA!
    - Se vejledningen der åbner for ping sidst i dokumentet her ☺
  - Det er vigtigt at 'Google' dokumenter til korrekt ASA software version for at finde de rette vejledninger ;-)
  - Udskift IP adresserne i denne vejledning med jeres egne efter behov!
  - Held og lykke ;-)

## Reset procedure



- Factory defaults reset procedure:
  - `asa>en`
  - `asa#conf t`
  - `asa(config)#config factory-default`
  - Vent på at konfigurationen er færdig og lav så en `reload`
  - Vent på at ASA'en er klar igen

## Korrektion af VLAN2 IP mm.



- Ny statisk IP adresse til VLAN2 (Outside):
  - `asa(config)#int vlan2`
  - `asa(config-if)#ip address 192.168.63.35 255.255.255.0`
  - `asa(config-if)#exit`
- Ny statisk route til gateway of last resort:
  - `asa(config)#route outside 0.0.0.0 0.0.0.0 192.168.63.1`
- Slet de gamle NAT regler:
  - `asa(config)#no object network object_any`

## Konfiguration af nyt VLAN3



- Oprettelse af ekstra VLAN3 til DMZ:
  - `asa(config)#int vlan3`
  - `asa(config-if)#no forward interface Vlan1`
  - `asa(config-if)#nameif dmz`
  - `asa(config-if)#security-level 50`
  - `asa(config-if)# ip address 10.0.0.1 255.255.255.0`
  - `asa(config-if)# exit`
  - `asa(config)#`

## Konfiguration af port til DMZ



- Tilslutning af port 2 til VLAN3/DMZ:
  - `asa(config)#interface Ethernet0/2`
  - `asa(config-if)#switchport access vlan 3`
  - `asa(config-if)#exit`
  - `asa(config)#`

## Opsætning af DHCP i DMZ



- en del af mercantec\*

- Konfiguration af DHCP i DMZ-zonen:
  - `asa(config)#dhcpd address 10.0.0.100-10.0.0.150 dmz`
  - `asa(config)#dhcpd dns 192.168.63.1 interface dmz`
  - `asa(config)#dhcpd enable dmz`
- Tips: Husk at gemme running-config indimellem:
  - `asa(config)exit`
  - `asa#write`

## Opsætning af NAT/PAT



- en del af mercantec\*

- Konfiguration af LAN mod Internet NAT:
  - `asa(config)#object network inside-subnet`
  - `asa(config-network-object)#subnet 192.168.1.0 255.255.255.0`
  - `asa(config-network-object)#nat (inside,outside) dynamic interface`
- Konfiguration af DMZ mod Internet NAT:
  - `asa(config)#object network dmz-subnet`
  - `asa(config-network-object)#subnet 10.0.0.0 255.255.255.0`
  - `asa(config-network-object)#nat (dmz,outside) dynamic interface`

## Tillad 'ping' (ICMP) gennem ASA



- en del af **mercantec**

- Konfiguration af 'ping'-policy på ASA5505:
  - `ASA(config)# class-map icmp-class`
  - `ASA(config-cmap)# match default-inspection-traffic`
  - `ASA(config-cmap)# exit`
  - `ASA(config)# policy-map icmp_policy`
  - `ASA(config-pmap)# class icmp-class`
  - `ASA(config-pmap-c)# inspect icmp`
  - `ASA(config-pmap-c)# exit`
  - `ASA(config)# service-policy icmp_policy interface outside`