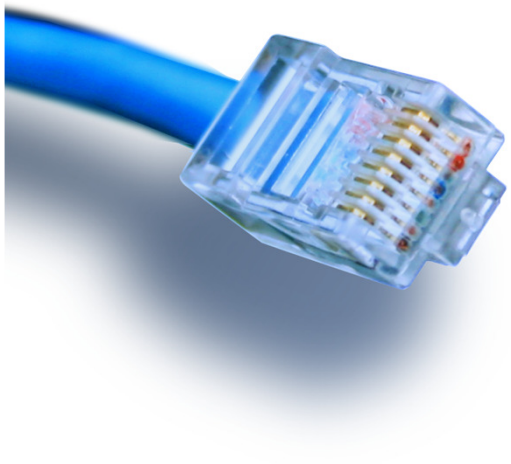
HOUSE OF TECHNOLOGY

– en del af mercantec



Cisco ASA 5505

Vejledning

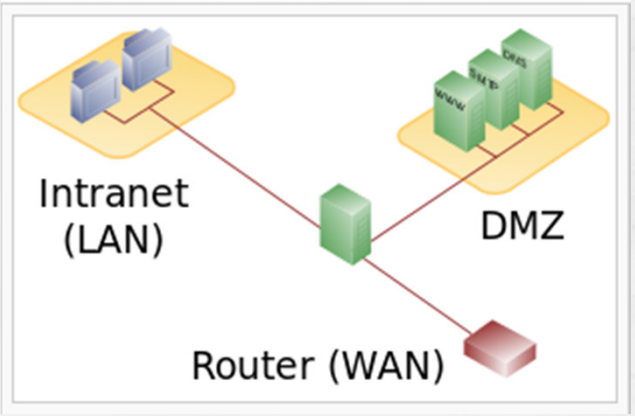
Opsætning af DMZ-zone

Hvad er en DMZ-zone???

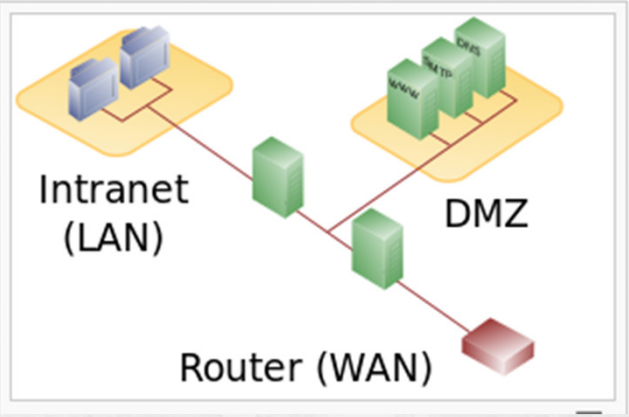
HOUSE OF TECHNOLOGY

– en del af mercantec

- En ‘demilitariseret zone’ eller ‘ingen mands land’! ☺
  - http://en.wikipedia.org/wiki/DMZ_%28computing%29

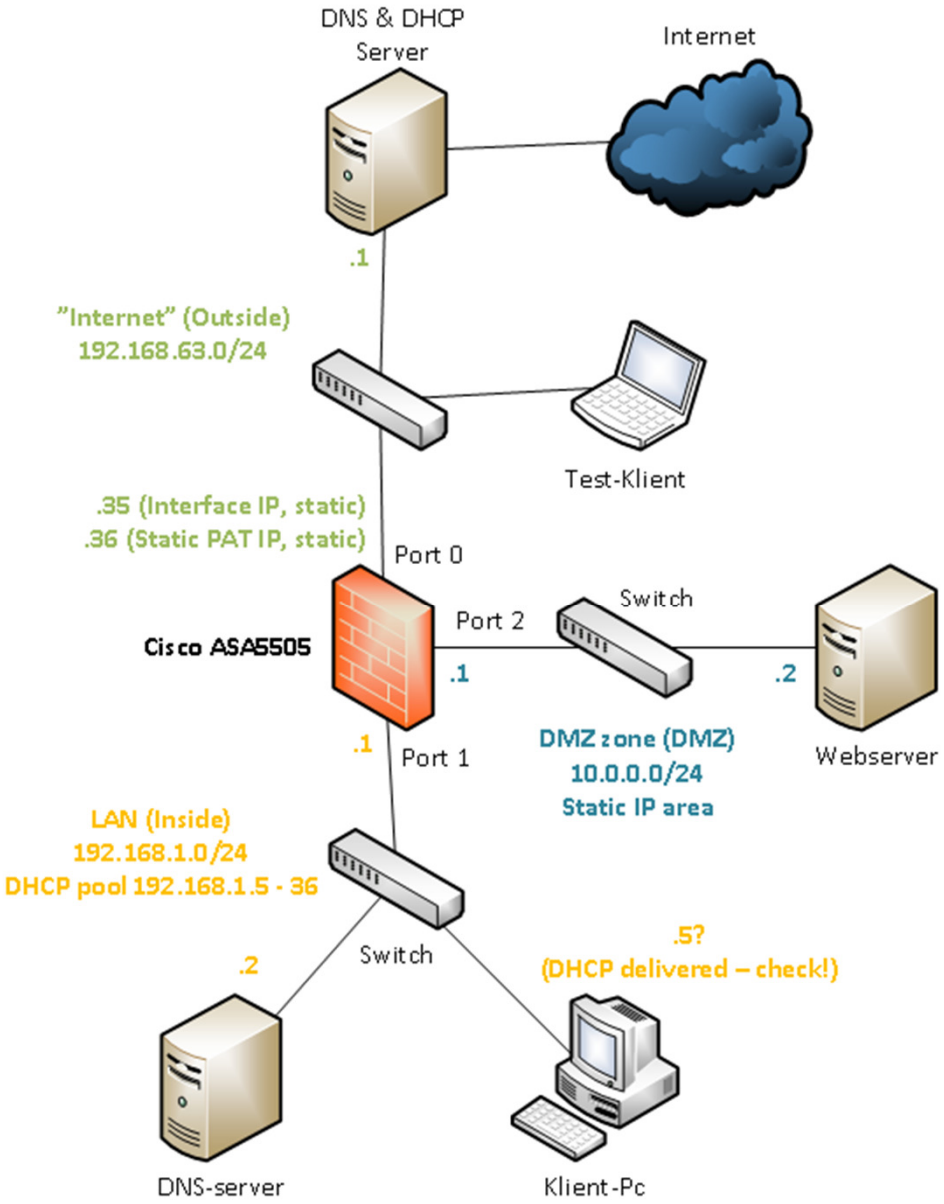


3-legged network DMZ



Dual firewall DMZ

Målet for vores ASA netværk:



HOUSE OF TECHNOLOGY

– en del af mercantec

- 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 på de næste sider ☺
  - 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

HOUSE OF TECHNOLOGY

– en del af mercantec

- 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

Tillad ‘ping’ (ICMP) gennem ASA

HOUSE OF TECHNOLOGY

– en del af mercantec

- Konfiguration af tillad ‘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

Korrektion af VLAN2 IP mm.

HOUSE OF TECHNOLOGY

– en del af mercantec

- 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 obj_any

Konfiguration af nyt VLAN3

HOUSE OF TECHNOLOGY

– en del af mercantec

- Oprettelse af ekstra VLAN3 til DMZ:
  - asa(config)#int vlan3
  - 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

HOUSE OF TECHNOLOGY

– en del af mercantec

- 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

HOUSE OF TECHNOLOGY

– en del af mercantec

- Konfiguration af DHCP i DMZ-zonen:
  - asa(config)#dhcpd address 10.0.0.100-10.0.0.131 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 dynamisk NAT/PAT

HOUSE OF TECHNOLOGY

– en del af mercantec

- Konfiguration af LAN mod Internet Dynamisk 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 Dynamisk 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

Definer extern webserver adresse

HOUSE OF TECHNOLOGY

– en del af mercantec

- Konfiguration af nyt object til extern webserver ip adresse:
  - asa(config)#object network webserver_external_ip
    - Host 192.168.63.36
  - Denne adresse skal vælges enten som en IP range eller en host IP. I dette tilfælde vælges blot en enkelt host adresse, 192.168.63.36. Den skal naturligvis være ledig ☺
  - For at externe klienter senere kan 'ramme' vores service skal den valgte adresse naturligvis være én som routes hen til vores offentlige ip på Outside interfacet.

Tillad HTTP trafik ind i DMZ

HOUSE OF TECHNOLOGY

– en del af mercantec

- ACL der tillader Webserver port 80 tcp trafik ind i DMZ:
  - Der oprettes et specielt network object til port 80 PAT:
    - asa(config)#object network webserver_internal_ip_port_80
      - host 10.0.0.2
  - Der oprettes en ACL der tillader port 80 trafik ind på DMZ:
    - asa(config)#access-list outside_acl extended permit tcp any object webserver_internal_ip_port_80 eq www
  - Den nye ACL knyttes til interface Outside i retning IN:
    - asa(config)#access-group outside_acl in interface outside

Statisk PAT af port 80 til DMZ

HOUSE OF TECHNOLOGY

– en del af mercantec

- Statisk PAT-regel af port 80 TCP trafik ind til server i DMZ:
  - Der oprettes et specielt network object til port 80 PAT:
    - asa(config)#object network StaticPAT_Out_DMZ_Port80
      - host 192.168.63.36
      - nat (dmz,outside) static webserver_external_ip service tcp www www

Tillad HTTPS trafik ind i DMZ

HOUSE OF TECHNOLOGY

– en del af mercantec

- ACL der tillader Webserver port 443 tcp trafik ind i DMZ:
  - Der oprettes et specielt network object til port 443 PAT:
    - asa(config)#object network webserver_internal_ip_port_443
      - host 10.0.0.2
  - Der oprettes en ACL der tillader port 443 trafik ind på DMZ:
    - asa(config)#access-list outside_acl extended permit tcp any object webserver_internal_ip_port_443 eq www
  - ACL'en er allerede knyttet til interface Outside i retning IN, så her behøver vi ikke gøre mere.

Statisk PAT af port 443 til DMZ

HOUSE OF TECHNOLOGY

– en del af mercantec

- Statisk PAT af port 443 TCP trafik ind til server i DMZ:
  - Der oprettes et specielt network object til port 443 PAT:
    - object network StaticPAT_Out_DMZ_Port443
      - host 192.168.63.36
      - nat (dmz,outside) static webserver_external_ip service tcp https https
  - Bemærk:
    - Husk at gemme = write ☺

Tillad DNS fra DMZ til LAN

HOUSE OF TECHNOLOGY

– en del af mercantec

- Eksempel: ACL der tillader port 53 tcp trafik fra DMZ til LAN:
  - asa(config)#object network dns-server
  - asa(config-network-object)#host 192.168.1.3
  - asa(config-network-object)#exit
  - asa(config)#access-list dmz_acl extended permit udp any object dns-server eq domain
  - asa(config)#access-list dmz_acl extended deny ip any object inside-subnet
  - asa(config)#access-list dmz_acl extended permit ip any any
  - asa(config)#access-group dmz_acl in interface dmz