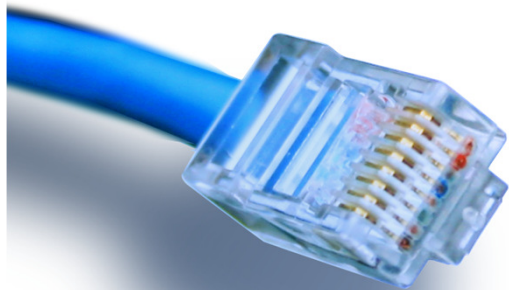


HOUSE OF
TECHNOLOGY



- en del af **mercantec**⁺



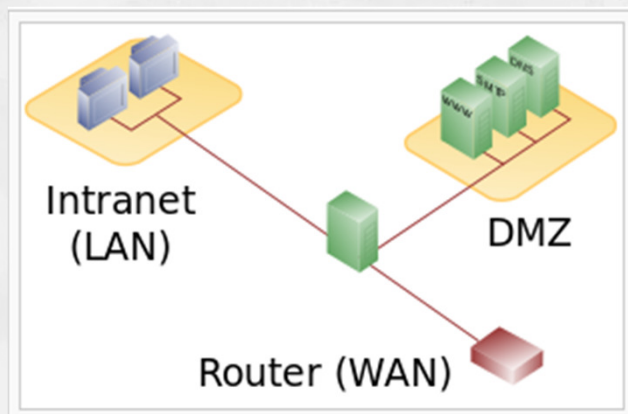
Cisco ASA 5505

Vejledning

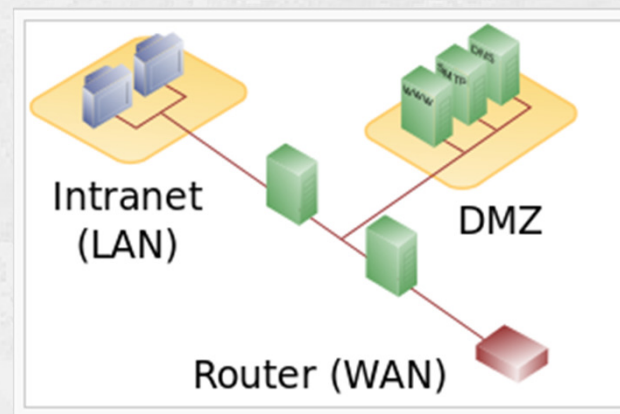
Opsætning af DMZ-zone

Hvad er en DMZ-zone???

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

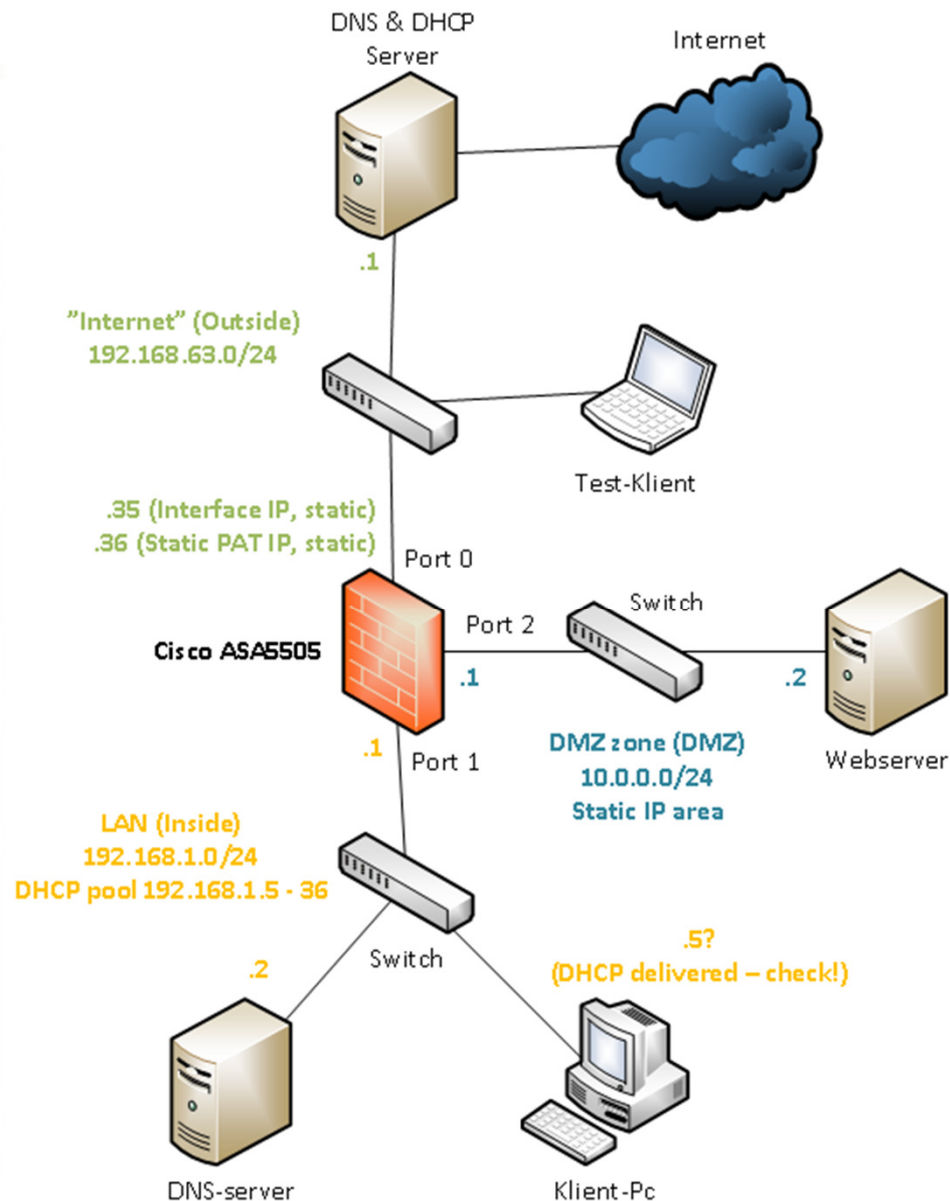


3-legged network DMZ



Dual firewall DMZ

Målet for vores ASA netværk:



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

Bemærk!

- 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

- 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

- 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.

- 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)#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

- 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`

- 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`

Tillad HTTP trafik ind i DMZ

- ACL der tillader Webserver port 80 tcp trafik ind i DMZ:
 - `asa(config)#object network webserver`
 - `host 10.0.0.2`
 - `asa(config)#access-list outside_acl extended permit tcp any object webserver eq www`
 - `asa(config)#access-group outside_acl in interface outside`

Statisk PAT af port 80 til DMZ

- Statisk PAT-regel af port 80 TCP trafik ind til server i DMZ:
 - `asa(config)#object network StaticPAT_Out_DMZ_Port80`
 - `host 192.168.63.36`
 - `object network webserver`
 - `host 10.0.0.2`
 - `nat (dmz,outside) static StaticPAT_Out_DMZ_Port80 service tcp www`
`www`
 - Bemærk:
 - Der oprettes et specielt network object til port 80 PAT

Tillad HTTPS trafik ind i DMZ

- Rettelse af ACL `outside_acl`, så den også tillader HTTPS:
 - `asa(config)#access-list outside_acl extended permit tcp any object webservers eq https`
- ACL `outside_acl` er allerede tilknyttet interface `outside`, så her behøver vi ikke gøre mere.

Statisk PAT af port 443 til DMZ

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

Tillad DNS-trafik fra DMZ til LAN

- ACL der tillader DNS 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`