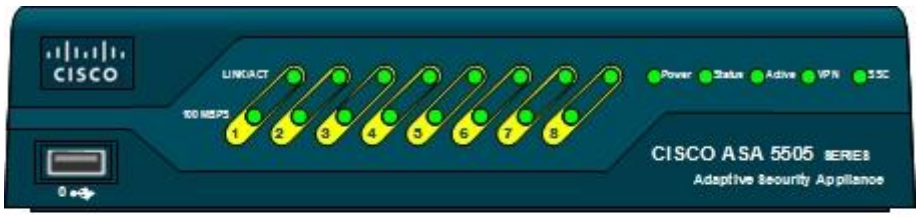
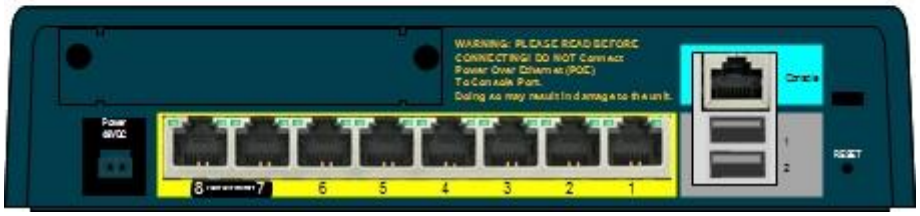
Opgave 1

Cisco ASA 5505 grundkonfiguration.



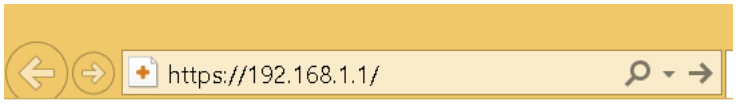


Indhold

ASA konfiguration

Forbind ASA port 0 til Internettet og port 1 til din PC. ASA'en har indbygget en DHCP server på 192.168.1.0/24 nettet som giver PC'en IP adresse. Check eventuelt med IPCONFIG kommandoen.

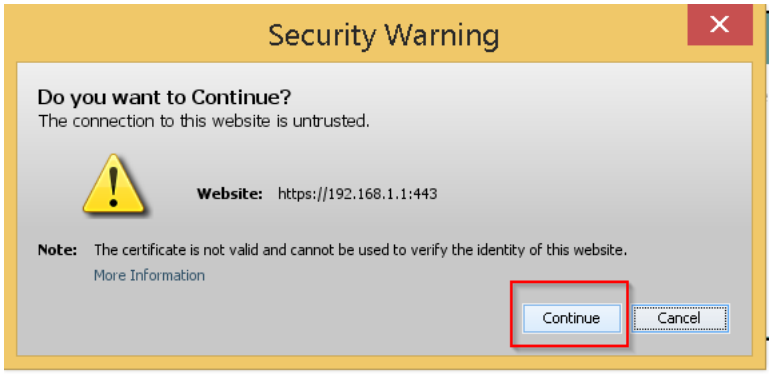
Start Internet Explorer og tilgå ASA med https://192.168.1.1



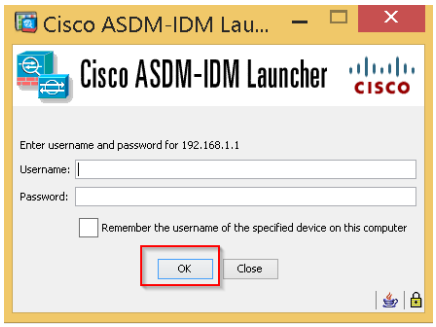
Figur 1 - Fra Internet Explorer start session til https://192.168.1.1

Figur 2 - Da der ikke er et trusted sikkerheds certifikat bliver vi nødt til at fortælle at vi stoler på ASA'en

Figur 3 - Start ASDM



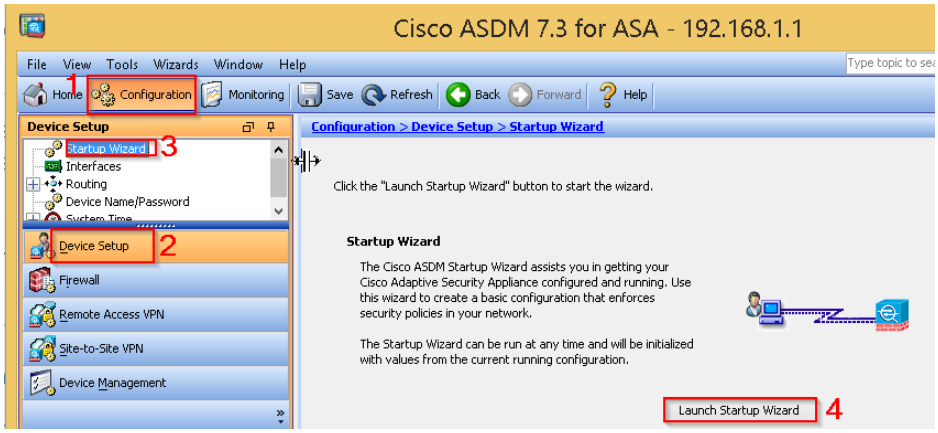
Figur 4 - Og ja vi stoler på certifikatet



Figur 5 - der er ikke oprettet brugere endnu - så <OK> får os ind

Figur 6 - Vi leger kun - så vi enabler ikke Smart Call Home

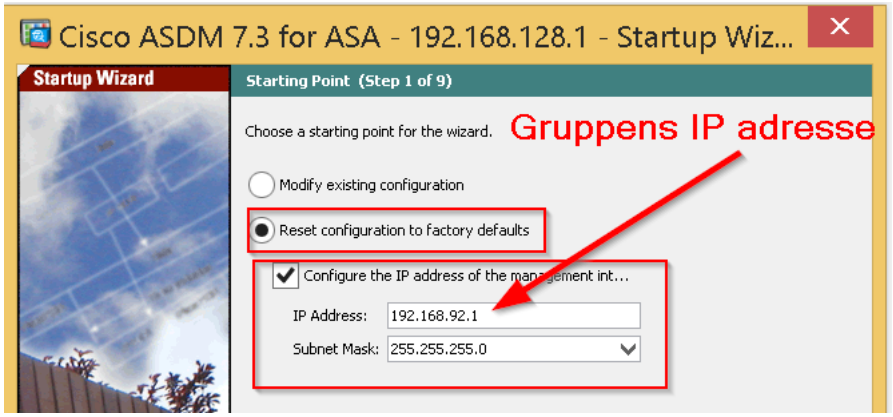
Startup Wizard



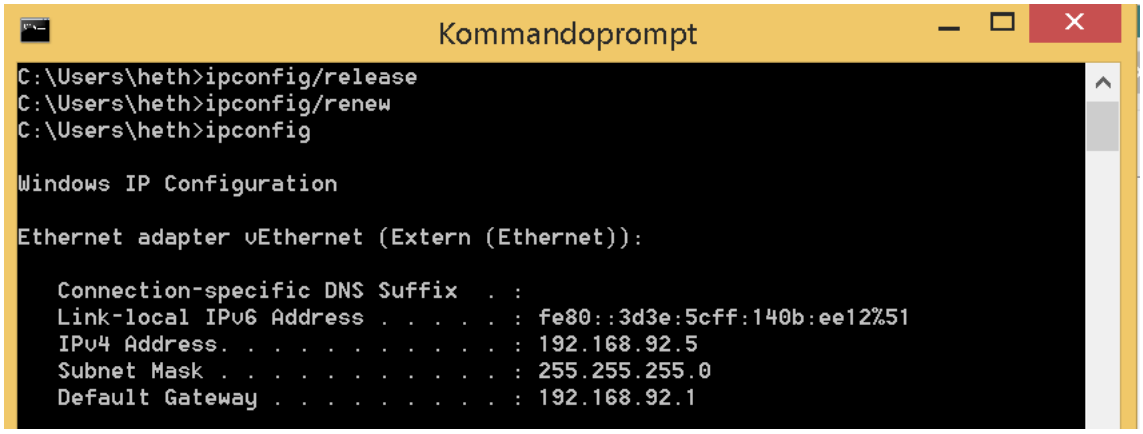
Figur 7 - Kør "Startup-Wizard"

Vi ønsker at ændre grundlæggende konfiguration til gruppens logiske IP netværk¨

HUSK: Det er gruppens ip adresse der skal anvendes.



ASA'en vil herefter resette til factory default og genstarte. Det tager nogle minutter og forbindelsen til ASA'en mistes fordi den får en ny IP adresse.

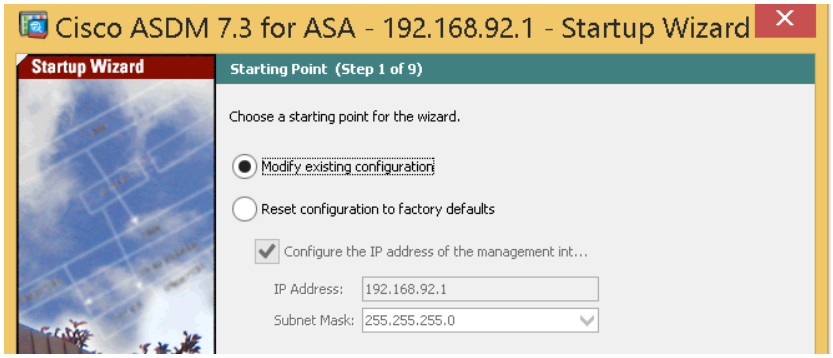


Figur 8 - Ny ip adresse hentes fra omkonfigurerede ASA

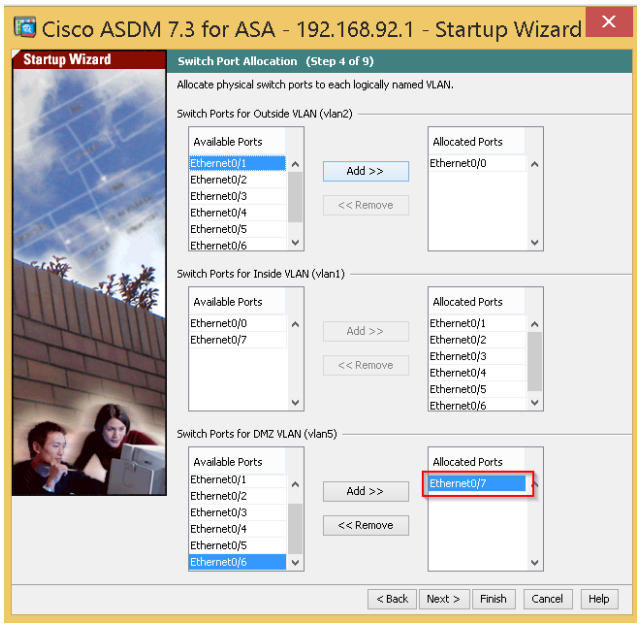
Konfiguration med ny IP adresse

Start ASDM igen med den nye IP adresse og kør ***Startup Wizard*** igen. Der er i alt 9 steps i Wizarden.

Bemærk: Steps der ikke er vist i anvisningen skal ikke ændres fra default!

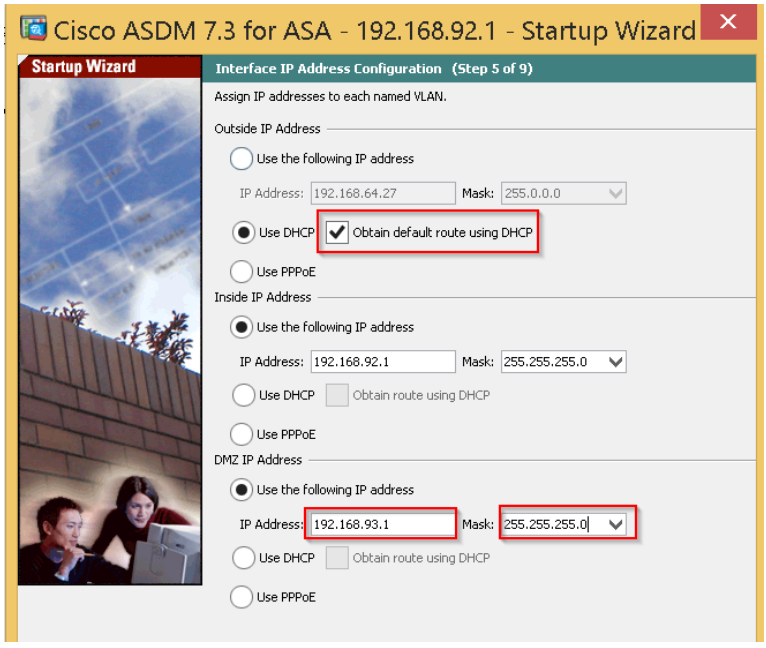


Figur 9 - Denne gang ændrer vi den eksisterende konfiguration

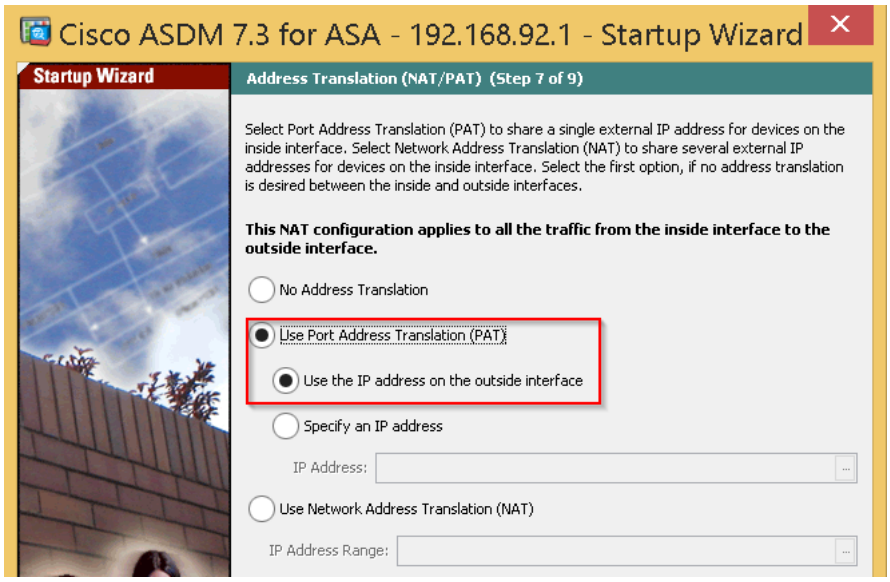


Figur 10 - I step 4 tilføjes Eternet0/7 til DMZ VLAN'et

DMZ VLAN'et tildeles IP adressen 192.168.[gruppens IP + 1].1 og subnet masken 255.255.255.0. Husk at markere ***Obtain default route using DHCP***



Figur 11 – I step 5 IP adresse tildeles DMZ og default route fås fra DHCP



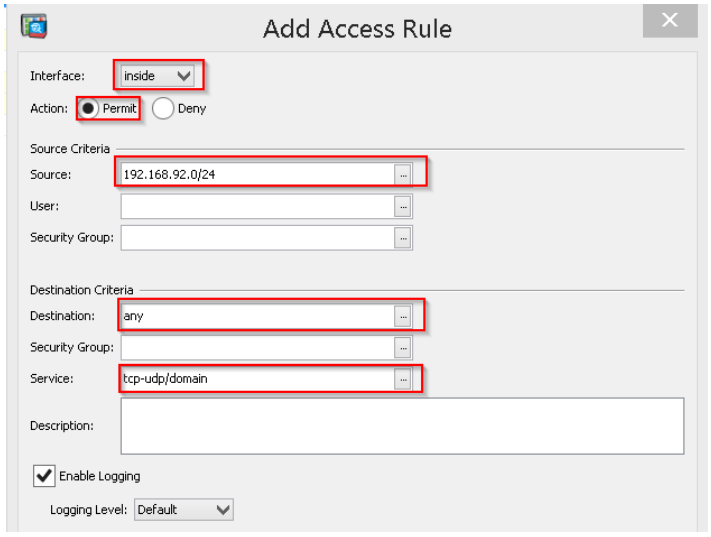
Figur 12 - I Step 7 startes NAT

Afslut Wizarden med ***Finish*** i step 9.

Oprettelse af firewall regler

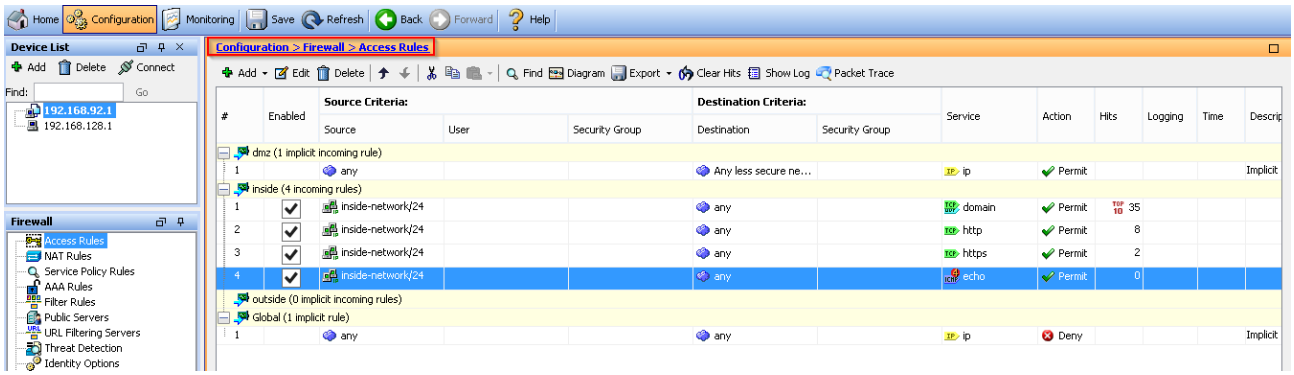
I dette eksempel ønsker vi at tillade trafik fra inside netværket til

- TCP/UDP port 53 – DNS trafik
- TCP port 80 – HTTP trafik
- TCP port 443 – HTTPS trafik
- ICMP echo – ping pakker



Figur 13 - Eksempel på access rule TCP/UDP trafik til DNS

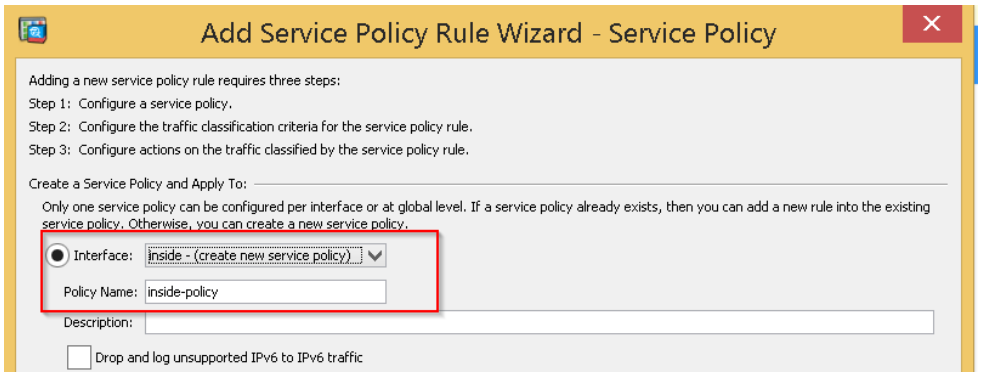
BEMÆRK: Ændringer bliver først overført til ASA'en når der trykkes på ***Apply***



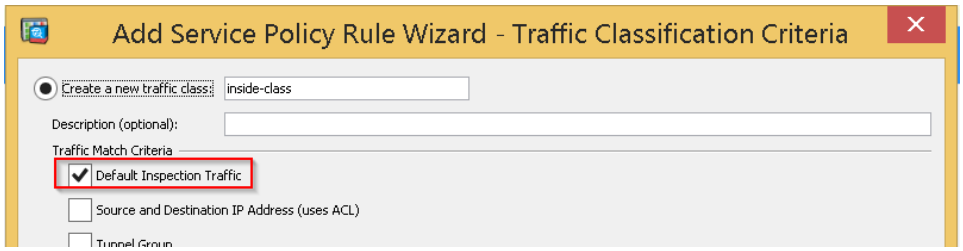
Figur 14 - Regler oprettet i Access Rules

Nu burde DNS, HTTP og HTTPS fungere. Ping fungerer ikke endnu da firewallen ikke tillader returpakkerne at komme tilbage igennem firewallen. Ping pakkerne kommer fint ud men pong pakkerne bliver spærret af firewallen.

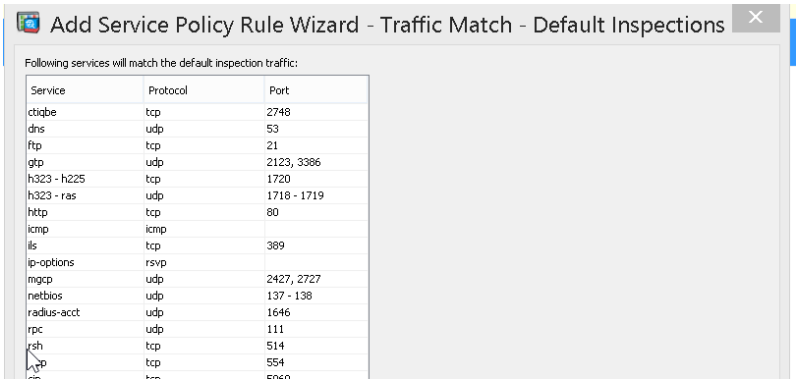
For at tillade pong pakkerne at komme ind skal der laves en ***inspect*** regel der tillader de associerede pong pakker at komme ind. Ved TCP og UDP trafik associaserer firewallen trafikken baseret på IP adresse par og port numre.



Figur 15 - Tilføj Service Policy i Configuration-->Firewall-->Service Policy Rules

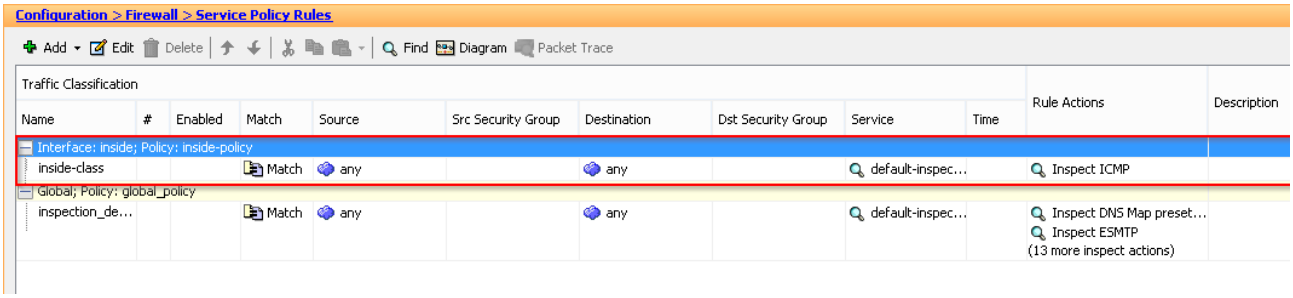


Figur 16 - Vi ønsker at standard inspektion af ICMP trafik

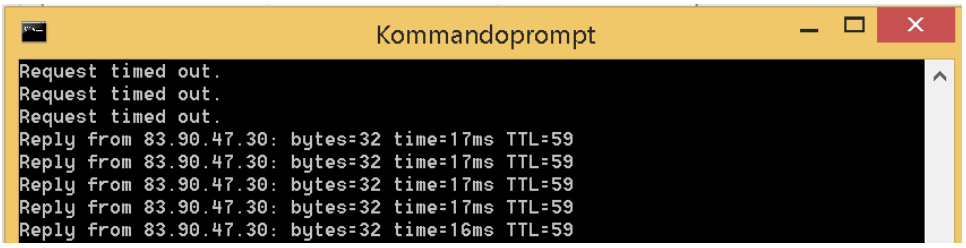


Figur 17 – Liste over standard services der kan inspiceres

Figur 18 - ICMP markeres til Inspektion



Figur 19 - Service Policy tilføjet



Figur 20 - Efter at have trykket "Apply" kommer returtrafikken fint igennem

BEMÆRK: ASA'en gemmer først konfigurationen i non-volatile memory når der trykkes på ***Save***