

6105 Windows Server og datanett

Labøving 10b: NAT og portforwarding i VirtualBox

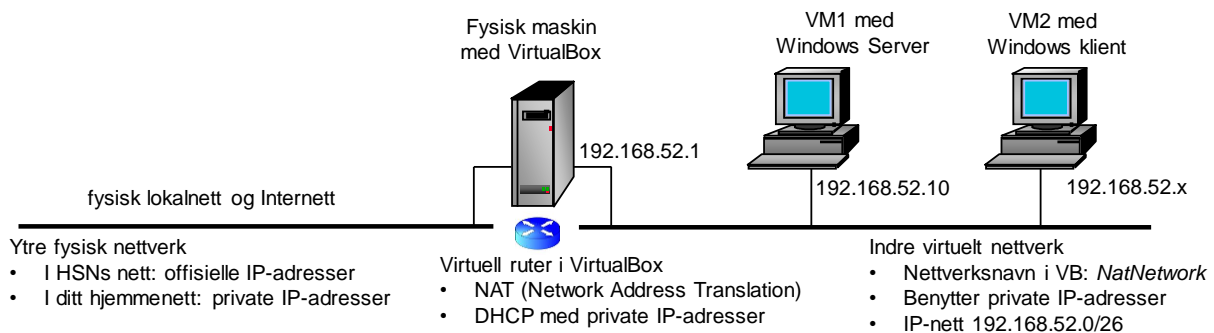
Forkunnskaper og forutsetninger

Du bør se gjennom leksjon 10 *Nettverkskomponenter* før du gjør denne øvingen.

Introduksjon

Denne leksjonen viser hvordan du kan bruke mekanismen *portforwarding* for å gi klienter utenfor en NAT-ruter, tilgang til tjenere og tjenester på innsiden av rutere. Dette er en mekanisme som brukes en del i internetbaserte spill, men den er også relevant for andre nettverksapplikasjoner.

Nettverkskonfigurasjonen for "laboppsettet" på den fysiske maskinen din ser ut som i figuren nedenfor:



- De to virtuelle maskinene er koblet i et virtuelt nettverk i VirtualBox (*NatNetwork*).
- VirtualBox på den fysiske maskinen fungerer som en **ruter** med NAT mellom det indre virtuelle nettet og det ytre fysiske nettet.
- Ruterens i VirtualBox er koblet både til det fysiske nettet og det virtuelle nettet. På "innsiden" har ruterens en IP-adresse (192.168.52.1) i IP-nettet for det virtuelle nettet. I det fysiske nettet har den samme IP-adresse som den fysiske maskinen din.

Dette oppsettet er svært likt det du vil ha i et hjemmenett som er koblet til Internett via en ruter med NAT fra internettleverandøren (ISP'en) din. Hjemmeruterens din vil da ha en offentlig IP adresse i ISP'ens nett på yttersiden. Det indre nettet bruker private IP-adresser, og NAT i hjemmeruterens oversetter disse til ruterens offentlige IP-adresse i det ytre nettet.

Med et standard NAT-oppsett kan klienter i det **indre** nettet å kontakte tjenere i det **ytre** nettet, men **ikke** omvendt. Vi skal nå se hvordan du kan konfigurere NAT-ruterens i VirtualBox med *portforwarding* slik at det også blir mulig å kontakte tjenere i det **indre** nettet fra klienter i det **ytre** nettet.

Oppgave a. Sjekke at standard NAT ikke gir tilgang fra ytre nett

1. Bruk **ipconfig** (Windows) eller **ifconfig** (Mac/Linux) på den **fysiske** maskinen og finn IP-adressen til den **fysiske** maskinens i det **ytre**, fysiske nettet (*Local Area Network*).
2. Start den virtuelle tjenermaskinen din og logg inn som **Administrator**.
3. Bruk en webleser på den **fysiske maskinen** og slå opp:
 - a. IP-adressen til din **fysiske** maskin i det **ytre** fysiske nettet.
 - b. IP-adressen til VirtualBox (på fysisk maskin) i det **indre** virtuelle nettet (*http://192.168.52.1*)
 - c. IP-adressen til din *virtuelle tjener* (*http://192.168.52.10*) der webtjeneren din kjører.

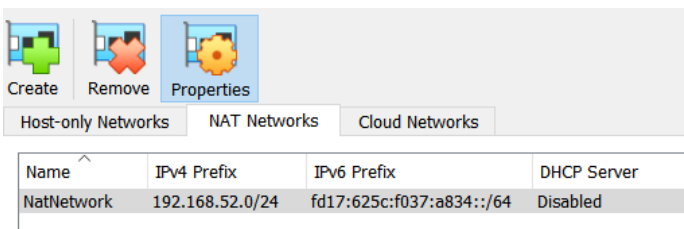
Du skal **ikke** få noe svar fra noen webtjener i noen av de tre tilfellene.


Forklaring: Den virtuelle tjenermaskinen med IIS står i et IP-nett bak NAT-ruteren i VirtualBox. TCP-forbindelser kan ikke etableres fra en maskin på utsiden til innsiden. Selv om ruteren på den fysiske maskinen også har et nettkort i det indre nettet, tillater ikke VirtualBox at den fysiske maskinen får tilgang til det indre nettet direkte via dette kortet. For VB er den fysiske maskinen kun tilkoblet det ytre fysiske nettet.

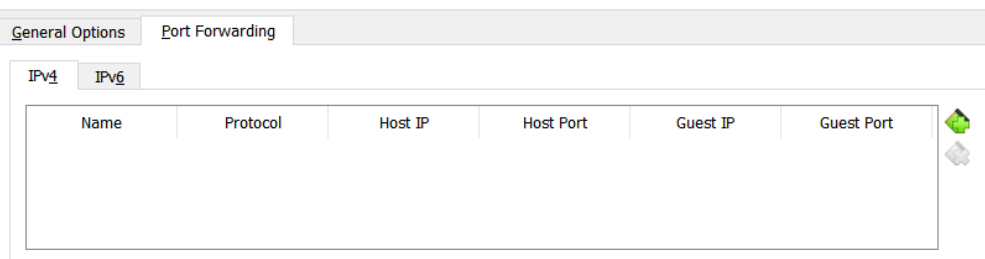
Oppgave b Portforwarding i VirtualBox


NAT-ruteren i VirtualBox gir mulighet for statisk videresending basert på portnummer (*portforwarding*). I denne øvingen skal du konfigurere *portforwarding*, slik at det blir mulig å kontakte tjenere på **innsiden** av ruteren fra klienter i nettet på **utsiden**.

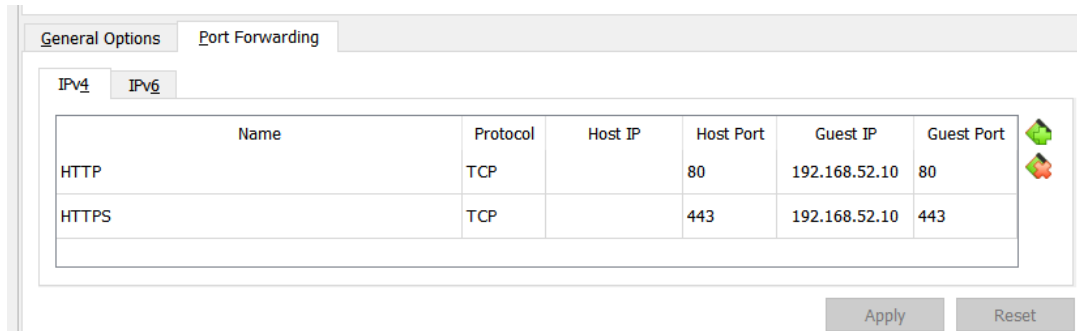
1. Velg **Tools** → **Network** i VirtualBox
2. Valg fanen *NAT Networks* og markèr nettet med navn *NatNetwork*





3. Bruk **Properties**-knappen  og velg fanen *Port Forwarding* nederst i bildet.



4. Bruk knappen  (*Adds new port forwarding rule*)
5. Lag en ny regel for å videresende http-trafikk (TCP-pakker adressert til port 80) til den virtuelle tjeneren din.
 - La feltet *Host IP* stå tomt. Da gjelder regelen for alle IP-adresser på den fysiske maskinen.
 - Bruk IP-adressen til tjenermaskinen din *som Guest IP*
6. Lag en tilsvarende ny regel for videresending av **https**-trafikk (pakker til port 443) til den virtuelle tjeneren din.



Name	Protocol	Host IP	Host Port	Guest IP	Guest Port	
HTTP	TCP		80	192.168.52.10	80	
HTTPS	TCP		443	192.168.52.10	443	

7. Klikk **OK** til du er tilbake i hovedbildet i *Oracle VM VirtualBox Manager*

NAT i VirtualBox er nå konfigurert for å tillate klienter i det fysiske nettet å kontakte webtjeneren i det virtuelle nettet. Test dette først fra den fysiske maskinen der du kjører VirtualBox:

8. Start webleseren på den **fysiske maskinen** og slå opp disse adressene (Den virtuelle tjeneren må fortsatt være på):
 - a. IP-adressen til din **fysiske** maskin i det **ytre** nettet.
 - b. IP-adressen til VirtualBox (fysisk maskin) i det **indre** virtuelle nettet (192.168.52.1)
 - c. IP-adressen til din *virtuelle tjener* (*http://192.168.52.10*) der webtjeneren kjører.

Nå bør du få svar i a.

VirtualBox gir imidlertid ikke fysisk maskin direkte tilgang til det virtuelle nettet. Derfor vil b. og c. ikke gi svar nå heller.

Oppgave c Teste portforwarding fra andre enheter i ytre nett

Du kan også teste at portforwardingen fungerer fra en **annen** fysisk enhet (PC/Mac, nettbrett eller mobiltelefon) som er koblet i samme fysiske nett som maskinen med VB, f.eks. hjemmenettet ditt. Dette forutsetter imidlertid at den lokale brannmuren på den **fysiske** maskinen som kjører VirtualBox ikke blokkerer innkommende pakker fra det fysiske nettet.

1. Skru **av** den lokale brannmuren (eller åpne port 80) på den **fysiske** maskinen med VirtualBox.
 - I *Windows* skrur du av brannmuren på fysisk maskin som forklart i labøving 10a *Windows brannmur*.
 - I *macOS* kan gjøre dette under **Systemvalg** → **Sikkerhet og personvern** → **Brannmur (System Preferences → Security & Privacy → Firewall)**
Se også supportsiden [OS X: Om programbrannmuren](#) fra Apple.



2. Start en webleser på en annen **fysisk enhet** og slå opp den **ytre** IP-adressen til din **fysiske** maskin (som kjører VirtualBox).

Portforwardingen i VirtualBox skal nå videresende http-forspørselen til webtjeneren på Windows Serveren din og du bør få svar fra denne.

Slutt på denne øvingen