6105 Windows Server og datanett

Labøving 10a: Windows brannmur

Forkunnskaper og forutsetninger

Du bør se gjennom leksjon *10 Nettverkskomponenter* før du gjør denne øvingen. Du må også ha gjennomført labøving *9a Installere og konfigurere webtjeneren IIS* før du starter på denne.

Introduksjon

I Windows Server vil installasjon av nye komponenter og programmer kunne endre konfigurasjonen av brannmuren automatisk. I denne øvingen skal du lære å konfigurere Windows Firewall på Windows Server manuelt. Du skal også teste at endringene i brannmuren fungerer som forventet.

Læringsmål:

- Kunne konfigurere Windows Firewall with Advanced Security.
- Kunne lage brannmurregler for angitte portnummer eller enkeltprogrammer, og et angitt scope (nett/adresse).

Oppgave a: Teste kommunikasjon uten brannmur

1. Logg på **tjenermaskinen** din som lokal **Administrator**.
   - Bruk **Control Panel ► System and Security ► Windows Firewall** og sjekk at brannmuren er skrudd **av** på alle profiler.
   - Start **Internet Information Services (IIS) Manager**, og sjekk at *Default Web Site* er startet, og lytter på TCP-port nr 80. (Dette forutsetter at du har gjort labøving 9a.)
2. Logg på **klientmaskinen** med en din egen domenebruker:
   - Test at du får ping'et tjenermaskinen fra kommandovinduet.
   - Test at du kan slå opp websiden (default website) på IIS-tjeneren din.
   - Slett midlertidige Internet-filer / «loggen» (*clear history*) og lukk nettleseren
   - Test at du får tilgang til delte mapper på tjeneren din fra *File Explorer* (filbehandler).
   - Lukk *File Explorer*.
   - Logg av klientmaskinen

Oppgave b: Standardinnstillinger og unntak i Windows brannmur

På tjenermaskinen:

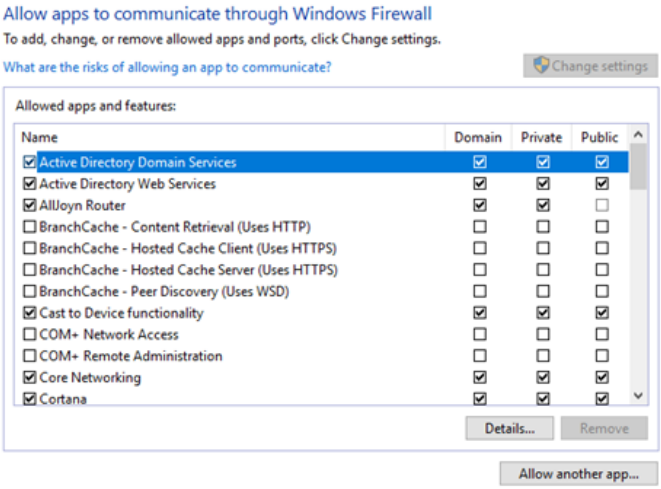
1. Bruk **Control Panel ► System and Security ► Windows Firewall**.
2. Klikk lenken Allow an app or feature through Windows Firewall
3. Hakene i listen viser hvilken nettverks-trafikk brannmuren vil slippe gjennom selv om den er skrudd på.

   Hva er status på følgende unntak:

   __ File and Printer Sharing

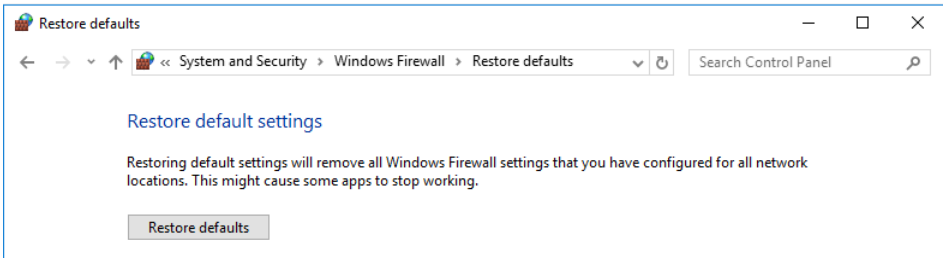
   __ World Wide Web Services (HTTP)

   __ Secure World Wide Web Services (HTTPS)



4. Gå tilbake og klikk lenken Restore defaults .

   Dette valget vil skru **på** brannmuren for alle profiler, og aktivere alle unntak som er standardinnstilling i Windows!



5. Sjekk på nytt listen over hvilken nettverkstrafikk brannmuren vil slippe gjennom.

   Hva er status på følgende unntak:

   ____ File and Printer Sharing

   ____ World Wide Web Services (HTTP)

   ____ Secure World Wide Web Services (HTTPS)

6. Lukk vinduet Windows Firewall.

På klientmaskinen:

7. Gjenta testene fra oppgave a. pkt.2 på klientmaskinen.

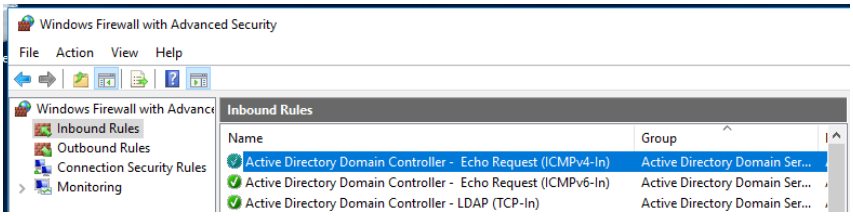
   Hvilke av testene fungerer fremdeles?_____

   Hvilke fungerer ikke? _____

Oppgave c: Konfigurere predefinert brannmurregel for ICMP (ping)

Kommandoen **ping** sender «*Echo Request*»-meldinger med kontrollprotokollen **ICMP**. Etter at AD er installert vil standardinnstillingene i Windows brannmur slippe gjennom slik **ICMP** trafikk. **ICPM** bruker ikke portnummer, men vi kan konfigurere brannmuren til å slippe gjennom / sperre hver enkelt av de ulike typene **ICMP**-meldingstypene.

1. Bruk tjenermaskinen og start **Windows Firewall with Advanced Security** fra **Tools** menyen i **Server Manager**.
2. Finn den **inngående** regelen *Active Directory Domain Controller (Echo Request ICMPv4-In)*. Hvis denne er grønn er denne regelen aktiv, dvs. at disse pakkene slipper gjennom.



3. Dobbeltklikk på regelen for å åpne egenskapsvinduet.

   Hvilken verdi har feltet *Action* på denne regelen? _____

4. Bruk fanene i egenskapsvinduet og svar på følgende:

   Hvilken *transportprotokoll* gjelder denne regelen for? _____

   Hvilke *portnummer* vil denne regelen åpne i brannmuren? _____

   Hvilket *scope* gjelder for denne brannmurregelen? _____

   Hva betyr dette scopet?_____

   Hvilke nettverksprofiler gjelder denne brannmurregelen for? _____

5. Velg fanen *General* og endre *Action* til **Block the connection** og klikk **Apply.**
6. Forsøk å **ping**e tjeneren fra klientmaskinen på nytt. Denne gangen bør du **ikke** få svar.
7. Endre Action tilbake til *Allow the connection* og trykk **Apply.**
8. Forsøk å **ping**e serveren fra klientmaskinen på nytt. Nå vil du få svar igjen.
9. Deaktiver regelen ved å fjerne haken i feltet ☐ Enabled. Nå vil du ikke får svar på ping.
10. Sett innstillingene på regelen tilbake til opprinnelig innstilling og sjekk at du da får pinget fra klienten.

Oppgave d: Lage portbaserte brannmurregler for http/https

Du skal nå definere en ny **portbasert** brannmurregel:

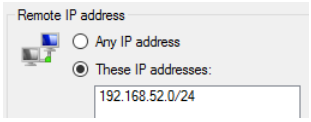
1. Bruk **Windows Firewall with Advanced Security** på tjenermaskinen.
2. **Sorter** reglene etter kolonnen *Name* og sjekk status på følgende inngående regler:

World Wide Web Services (HTTP Traffic-In)	World Wide Web Services (HTTP)	All	Yes
World Wide Web Services (HTTPS Traffic-In)	Secure World Wide Web Services (HTTPS)	All	Yes

   Disse skal være aktivert (grønt merke). Hvis ikke kan du aktivere dem.

   Hvilke *portnummer* åpner disse to reglene for? _____
3. Bruk en nettleser på *klientmaskinen* og slå opp hjemmesiden på web serveren din.
   Du bør få kontakt med webtjeneren.
4. Bruk **Internet Information Services (IIS) Manager** på *tjenermaskinen*:
   - Endre portnummer på nettstedet *Default Web Site* til 8080. (*Edit Bindings*)
   - Restart *Default Web Site* (ikke maskinen!)
5. På *klientmaskinen*:
   - Slett midlertidige internettsider (*Clear history / Delete log*)
   - Forsøk å slå opp hjemmesiden på web serveren på det nye portnummeret (**http://*servernavn*:8080**).

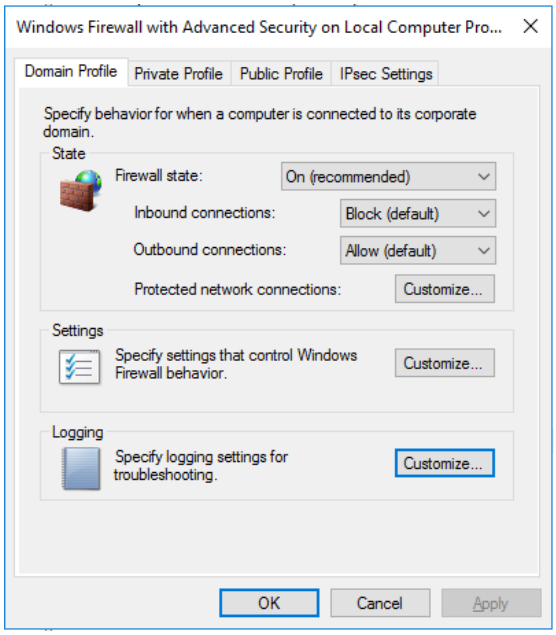
   Hvorfor får du ikke få kontakt med webtjeneren nå? _____
6. På *tjenermaskinen*:
   - Bruk **Windows Firewall with Advanced Security**
   - Lag en ny **inngående portbasert** regel som åpner for **TCP** port **8080**
   - Kall regelen **Webtrafikk på port 8080** og **aktiver** regelen.
   - Bruk fanen *Scope* og feltet *Remote IP adress.* Konfigurer scopet slik at webtilgang kun godtas fra maskiner i det virtuelle lokalnettet (IP-subnett: 192.168.52.0/24).

7. Fra *klientmaskinen*: Test at webtjeneren på port 8080 kan nås fra nettleseren nå.
8. Deaktiver den nye regelen på tjeneren og sjekk at du da ikke får slått opp websiden (etter at du har slettet midlertidige internettsider)
9. På *tjenermaskinen*:
   - Sett *Default Web Site* tilbake til standard port 80 og restart websiten
   - Slett den nye brannmurregelen for TCP port 8080.
10. Fra *klientmaskinen*: Sjekk at du får kontakt med websiden på standard port 80.

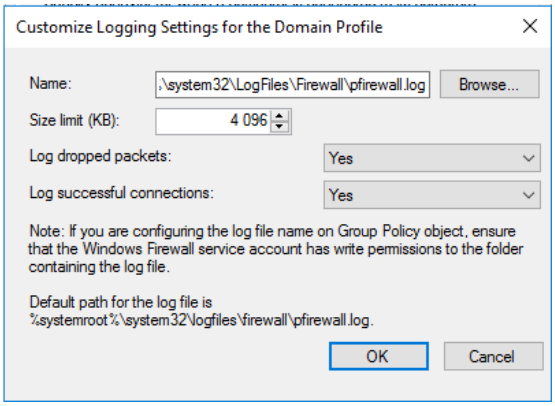
Oppgave e: Logging og scope for en brannmurregel

1. Bruk **Windows Firewall with Advanced Security** på *tjenermaskinen*
2. Høyreklikk symbolet
   Windows Firewall with Advanced Security on Local Computer
   øverst til venstre i vinduet, og velg **Properties**.
3. Velg fanen **Private Profile**
4. Bruk knappen **Customize…** bak *Logging.*



5. Skru på følgende logging:
   - *Log dropped packets*
   - *Log successful connections.*
6. Noter deg navn og plassering på loggfilen:

   _____
7. Lukk egenskapsvinduet med **OK**.

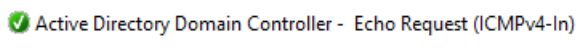


8. Finn den inngående reglen Active Directory Domain Controller - Echo Request (ICMPv4-In) , velg **Properties** og endre *Action* til **Block the connection**
9. På *klientmaskinen*:
   - Slå opp websiden på tjeneren. Det bør gå bra.
   - Forsøk å pinge tjeneren. Du skal ikke få svar.
10. På *tjenermaskinen*:
    - Åpne loggfilen for brannmuren i **Notepad** og studer innholdet.
    - Gå til slutten av filen og finn linjer med dagens dato og som indikerer at IP pakker fra klientmaskinen er **droppet** i brannmuren.

      Hvor mange slike linjer finner du? _____

Forklar betydningen av de enkelte verdiene i **en av** disse linjene:

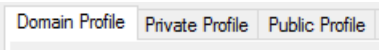
_____

- Lukk loggfilen.
- **Skru av** logging av *Log dropped packets* og *Log successful connections* i **Windows Firewall with Advanced Security**
- Åpne brannmuren for 

igjen.

Oppgave f: Avslutning av øvingen

For at brannmuren ikke skal hindre senere øvinger, skal du nå slå brannmuren på tjenermaskinen helt av (for alle profiler) før du avslutter denne øvingen:

1. Høyreklikk symbolet *Windows Firewall with Advanced Security* øverst til venstre i vinduet, og velg **Properties**.
2. Sett *Firewall state* til **Off** for alle tre profiler: 

3. Lukk **Windows Firewall with Advanced Security**

Slutt på denne øvingen