Windows Server 2012 — 14-Brandväggen

Denna laboration är en del av en serie labbar om Windows Server 2012R2 som till stor del bygger vidare på varandra. I denna laboration kommer vi att titta på brandväggen i Windows Server 2012 och få en bättre förståelse för hur den fungerar. Vi kommer att skapa egna regler i brandväggen och se hur det påverkar nätverkskommunikationen.

Antal: Enskilt eller i grupp om 2.

Material: Tillgång till SERVER1 och SERVER2 från tidigare laborationer.

Tips: Titta på relevanta genomgångar på webbplatsen http://itlararen.se/videos.html#video3

Utförande: SERVER1 och SERVER2 sitter på samma nätverk med fasta IP-nummer sedan tidigare laborationer.

1. Starta och logga in på SERVER2 som domänadministratör
2. Används **Server Manager** och klicka på **Add roles and Features** för att installera serverrollen **Web Server (IIS)**. Använd standardinställningar. Nu installeras webbservern IIS.
3. Använd **Server Manager** och klicka på **Local Server** i menyn till vänster.
4. Under **Properties**, alltså i fönstret till höger. Klicka på **IE Enhanced Security Configuration** och inaktivera detta för administratörer. Detta inaktiverar den extra säkerhetskonfigurationen som annars är aktiv och kan ställa till problem om man ska använda IE för att surfa på webben.
5. Starta **Internet Explorer** och verifiera att vi nu kan öppna standardsidan för IIS8 på vår server genom att ange **http://localhost** i adressfältet.
6. Logga in på SERVER1 som domänadministratör.
7. Inaktivera **IE Enhanced Security Configuration** för administratörer på samma sätt som I steg 4.
8. Starta **Internet Explorer** och verifiera att vi nu kan öppna standardsidan för IIS8 på SERVER2 genom att ange IP-adressen till SERVER2 i adressfältet **http://192.168.0.2**
9. Starta **Server Manager** och klicka på **Tools** och välj **Windows Firewall with Advanced Security** för att starta konsolen för avancerade brandväggsinställningar.
10. Högerklicka på högsta nivån i trädstrukturen till vänster som heter **Windows Firewall with Advanced Security on Local Computer** och välj **Properties**
11. Konfigurera inställningarna för **Domain Profile** så att utgående trafik (outbound connections) är **blocked** som standard och klicka på **OK** för att verkställa ändringarna. Dubbelkolla inställningar för nätverkskortet, har vi ej Internetanslutning så kan Windows Server få för sig att nätverket är *Public* och då får vi ändra profilen för Public så att utgående trafik blockeras.
12. Ta bort webbläsarhistoriken, snabbtangenten är **CTRL+SHIFT+DELETE** och klicka på **DELETE**.
13. Försök ansluta till SERVER2 igen via **http://192.168.0.2** eller klicka på **F5** för att uppdatera.
14. Verifiera att vi nu ej kan ansluta till webbservern. Detta då all utgående trafik blockeras vilket vi satt som standard och då görs detta om inga specifika brandväggsregler säger något annat.
15. Ändra tillbaka inställningarna för Domain Profile (och Public profile) så att utgående trafik (outbound connections) tillåts (Allow).
16. Använd Internet Explorer för att verifiera att vi nu återigen kan ansluta till SERVER2.
17. Tillbaka till **Windows Firewall with Advanced Security**. Högerklicka på noden **Outbound Rules** i menyn till vänster och välj **New Rule** för att starta **New Outbound Rule Wizard**.

18. Observera vilka valmöjligheter som finns. Välj **Port** och klicka på **Next**.
19. Välv **TCP** port **80** och klicka på **Next**
20. Under Action väljer vi standardalternativet **Block the Connection** och klicka på **Next**
21. Välj standardinställningarna vilket innebär att regeln aktiveras för alla nätverksprofiler. Klicka på **Next**
22. Ange ett beskrivande namn, t.ex. **Block TCP port 80** och klicka på **Finish** för att aktivera regeln.
23. Byt till Internet Explorer igen och ta bort webbläsarhistoriken (**CTRL+SHIFT+DELETE**)
24. Prova att ansluta till SERVER2 igen genom att uppdatera sidan (**F5**)
25. Verifiera att anslutningen blockeras av vår specifika regel.
26. Byt tillbaka till **Windows Firewall with Advanced Security** och högerklicka på regeln vi nyss gjorde och välj **Disable Rule** för att avaktivera regeln.
27. Byt tillbaka till Internet Explorer och prova att ansluta till SERVER2 igen genom att uppdatera sidan (**F5**)
28. Verifiera att vi återigen kan ansluta då vi inaktiverat blockeringen.
29. Tillbaka till **Windows Firewall with Advanced Security**. Högerklicka på noden **Outbound Rules** i menyn till vänster och välj **New Rule** för att starta **New Outbound Rule Wizard**.
30. Välj **Program** och klicka på **Next**
31. Ange sökvägen till Internet Explorer **C:\ProgramFiles (x86)\Internet Explorer\iexplore.exe** och klicka på **Next**
32. Under Action väljer vi standardalternativet **Block the Connection** och klicka på **Next**
33. Välj standardinställningarna vilket innebär att regeln aktiveras för alla nätverksprofiler. Klicka på **Next**
34. Ange ett beskrivande namn, t.ex. **Block Internet Explorer** och klicka på **Finish** för att aktivera regeln.
35. Byt till Internet Explorer igen och ta bort webbläsarhistoriken (**CTRL+SHIFT+DELETE**)
36. Prova att ansluta till SERVER2 igen genom att uppdatera sidan (**F5**)
37. Verifiera att anslutningen blockeras av vår specifika programregel.
38. Byt tillbaka till **Windows Firewall with Advanced Security** och högerklicka på regeln vi nyss gjorde och välj **Disable Rule** för att avaktivera regeln.
39. Byt tillbaka till Internet Explorer och prova att ansluta till SERVER2 igen genom att uppdatera sidan (**F5**)
40. Verifiera att vi återigen kan ansluta då vi inaktiverat blockeringen.

Detta skall du kunna efter genomförd labb:

- ✓ Skapa regler i Windows brandväggen
- ✓ Blockera eller tillåta anslutningar beroende på TCP/UDP port eller program
- ✓ Ändra standardinställningar för hur anslutningar ska hanteras