Windows Server 2012 — 15-IPSec

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 skapa *connection security rules* för att implementera IPsec kommunikation mellan SERVER1 och SERVER2.

Antal: Enskilt eller i grupp om 2.

Material: Tillgång till SERVER1 och SERVER2 från tidigare laboration.

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

Utförande: I denna laboration använder vi SERVER1 och SERVER2 från tidigare laborationer. Det går även bra att använda SERVER1 och CLIENT ifall man ej har tillgång till SERVER2. Från och med Windows Server 2008 och Windows Vista så har Windows inbyggt stöd för IPsec via brandväggen i Windows.

IPsec är ett samlingsnamn för flera protokoll som används för att säkra trafik med autentisering och kryptering. Detta sker i övre delen av lager 3 (Network Layer) vilket medför att all kommunikation som använder IPv4 eller IPv6 kan säkras utan att behöva ändra något i de övre applikationslagren.

1. Starta SERVER1 och logga in som domänadministratör
2. Starta **Server Manager** klicka på **Tools** och **Windows Firewall with Advanced security**
3. I trädstrukturen till vänster, högerklicka på **Connection Security Rules** och välj **New Rule** för att starta **New Connection Security Rule Wizard**
4. Under Rule Type välj **Server-to-Server** och klicka på **Next**
5. På Endpont page under **Which computers are in Endpoint 1** välj **These IP-addresses** och klicka på **Add**.
6. Mata in IP-numret för SERVER1 **192.168.0.1** och klicka på **Ok**
7. På Endpont page under **Which computers are in Endpoint 2** välj **These IP-addresses** och klicka på **Add**.
8. Mata in IP-numret för SERVER2 **192.168.0.2** och klicka på **Ok**
9. Klicka på **Next**
10. På sidan Requirements välj **Request Authentication for Inbound and Outbound connections** och klicka på **Next**
11. På sidan Authentication Method välj **Advanced** och klicka på **Customize**
12. Under First authentication, klicka på **Add** och välj **Preshared Key** (ej att rekommendera men för laborationen så väljer vi detta då det är enklast) och ange nyckeln **testnyckel** klicka på **Ok** två gånger och klicka på **Next**
13. Välj standardinställningar på sidan Profile och klicka på **Next**
14. Ange ett lämpligt namn, t.ex. **SERVER1 to SERVER2** och klicka på **Finish** för att skapa vår nya Connection Security Rule.
15. Välj noden **Connection Security Rules** under noden **Monitoring Mode** och verifiera att den nya regeln är aktiv (att den listas).
16. Starta en kommandotolk, exempelvis med **WIN+R** ange **CMD** och klicka på **Run**
17. Prova att kommunicera med IPSec (förhoppningsvis) genom att pinga SERVER2 med kommandot **ping 192.168.0.2**

18. Som ni ser så kan vi kommunicera med SERVER2 men hur vet vi ifall vi kommunicerar säkert via IPSec? Byt tillbaka till **Windows Firewall with Advanced Security** och markera noden **Windows Firewall with Advanced Security on Local Computer – Monitoring – Security Associations – Main Mode**. Vi ser nu att det inte listas någontig här. Hade en IPSec kommunikation upprättats så hade en SA (Security Association) skapats och listats här. För att IPSec kommunikation ska upprättas så måste vi konfigurera båda datorerna till att använda IPSec.
19. Byt till SERVER2 och logga in som domänadministratör.
20. Öppna **Windows Firewall with Advanced Security** (på samma sätt som tidigare)
21. I trädstrukturen till vänster, högerklicka på **Connection Security Rules** och välj **New Rule** för att starta **New Connection Security Rule Wizard**
22. Under Rule Type välj **Server-to-Server** och klicka på **Next**
23. På Endpont page under **Which computers are in Endpoint 1** välj **These IP-addresses** och klicka på **Add**.
24. Mata in IP-numret för SERVER2 **192.168.0.2** och klicka på **Ok**
25. På Endpont page under **Which computers are in Endpoint 2** välj **These IP-addresses** och klicka på **Add**.
26. Mata in IP-numret för SERVER1 **192.168.0.1** och klicka på **Ok**
27. Klicka på **Next**
28. På sidan Requirements välj **Request Authentication for Inbound and Outbound connections** och klicka på **Next**
29. På sidan Authentication Method välj **Advanced** och klicka på **Customize**
30. Under First authentication, klicka på **Add** och välj **Preshared Key** (ej att rekommendera men för laborationen så väljer vi detta då det är enklast) och ange nyckeln **testnyckel** klicka på **Ok** två gånger och klicka på **Next**
31. Välj standardinställningar på sidan Profile och klicka på **Next**
32. Ange ett lämpligt namn, t.ex. **SERVER2 to SERVER1** och klicka på **Finish** för att skapa vår nya Connection Security Rule.
33. Välj noden **Connection Security Rules** under noden **Monitoring Mode** och verifiera att den nya regeln är aktiv (att den listas).
34. Starta en kommandotolk, exempelvis med **WIN+R** ange **CMD** och klicka på **Run**
35. Prova att kommunicera med IPSec (förhoppningsvis) genom att pinga SERVER1 med kommandot **ping 192.168.0.1**
36. Som ni ser så kan vi kommunicera med SERVER1 men används IPSec nu? Byt tillbaka till **Windows Firewall with Advanced Security** och markera noden **Windows Firewall with Advanced Security on Local Computer – Monitoring – Security Associations – Main Mode**. Nu bör det finnas en SA (Security association) som listas och visar att IPSec kommunikation har skett mellan SERVER1 och SERVER2
37. Högerklicka på den SA som listas och väl **properties** undersök egenskaperna och stäng sedan fönstret.
38. Markera noden **Quick Mode** och högerklicka på den SA som listas där och välj **properties** för att undersöka egenskaperna. Stäng fönstret.

    För att implementera IPSec i sin organisation så är det bäst att använda sig av certifikat istället för en pre-shared key. Likaså kan vi göra motsvarande konfiguration av Windowsbrandväggen via Group Policy och på så sätt enkelt aktivera IPSec för alla eller vissa datorer i vårt nätverk. Vi kan också kräva att IPSec ska användas istället för som i labben då vi föreslår att använda IPSec och funkar inte det så kommunicerar vi ändå. Vi kan även skapa

specifika regler i brandväggen då vi enbart tillåter viss typ av trafik ifall den är "säker" d.v.s. använder IPSec. Exempelvis enbart tillåta säker DNS-kommunikation eller att alla domänanslutna datorer måste använda IPSec vid kommunikation med vår Default Gateway mm.

Detta skall du kunna efter genomförd labb:

- ✓ Säkra kommunikationen mellan två datorer med IPSec