Serverbaserad Brandvägg

I denna laboration kommer ni att installera och konfigurera en serverbaserad brandväggslösning.

Antal: Enskilt eller i grupper om 2.

Material: Ni behöver 2 datorer varav en dator med 2 nätverkskort samt uppkoppling mot Internet. Installationsmedia för vald brandväggslösning, en dator som används som klient (exempelvis med Windows 7 eller liknande) samt en dator som ni ska installera en brandväggslösning på. Det går bra att göra denna laboration virtuellt (då räcker det med en dator med VirtualBox eller Hyper-V samt Internetanslutning).

Bakgrund: Det finns flera anledningar till att man vill ha en fungerande brandvägg och fördelarna är många. Det finns idag ett flertal lösningar för att enkelt skapa sig en egen brandvägg ifall man har en dator över. De allra flesta lösningarna som baseras på Linux är gratis och har flera funktioner utöver brandväggen samt bra stöd för hårdvara. Lösningar som baseras på BSD är generellt mer resurssnåla men har sämre stöd för hårdvara. För Windows finns en massa brandväggslösningar som dock faller under kategori *personliga* brandväggar och som inte är till för en *router/gateway* exempelvis *ZoneAlarm* och *Windowsbrandväggen*. I denna laboration ska ni arbeta med en ***server-based firewall***. Med detta begrepp menar man en dator/server som används som en fristående brandväggslösning.

Översikt av olika lösningar

Lösning	Storlek	Kommentar
Smoothwall	~80MB	Linux. Gratis (express). Relativt enkel.
Devil Linux	~200MB	Linux. Gratis.
IPCop	~60MB	Linux. Gratis. Relativt enkel.
IPFire	~75MB	Linux.Gratis. Bygger på IPCop.
PfSense	~150MB	Linux. Gratis. Mycket funktioner.
ClearOS	~700MB	Linux. Gratis. F.d. *ClarkConnect*
Zentyal	~600MB	Linux. Gratis. F.d. *eBox*
Monowall	~6MB!	BSD-baserad. Extremt kompakt.
~~**ISA Server 2006**~~	~150MB	Microsoft. Windows Server - Fungerar bara på Server 2003/2003R2. Kostar. Underhålls ej.
~~**Forefront Threat Management Gateway (TMG)**~~	~1,2GB	Microsoft. För Windows Server 2008. Kostar. Underhålls ej längre.

OBS! Jag har valt att enbart ta upp ”färdiga” brandväggslösningar. Det går alldeles utmärkt att konfigurera valfri Linuxdistribution eller BSD-distribution (som Debian, Ubuntu, OpenBSD etc.) till att agera brandvägg.

Vanliga tillämpningar för brandväggar

- Skydda mot(oönskad) inkommande trafik. Paketfiltrering.
- Öka prestandan (i form av Proxy-tjänster)
- Begränsa vilken typ av trafik som tillåts
- Prioritera nätverkstrafiken beroende på vem, när och vad som skickar data (”traffic shaping”).

Hemsior & Hjälp

På hemsidan itlararen.se under kategorin "blandat och säkerhet" hittar ni videogenomgångar för att komma igång med de flesta distributionerna. För mer information och hjälp hänvisas till respektive hemsida/manual. Tänk på att använda manualer och instruktioner är kunskapskrav för de flesta gymnasiekurser inom ämnet.

http://en.wikipedia.org/wiki/List_of_router_or_firewall_distributions, https://www.pfsense.org

http://www.smoothwall.org/

Syfte: Syftet med laborationen är att lära sig att installera, konfigurera och administrera en kraftfull brandväggslösning för hemmanätverk eller mindre/medelstort företag.

Uppgift: Alla uppgifter och allt ni gör skall dokumenteras, gärna med skärmdumpar.
Ni ska implementera en brandväggslösning för ett mindre företag. Ni ska välja en brandväggslösning för detta ändamål. Ni ska ansluta er brandvägg så att företagets datorer (LAN) ansluter till Internet via den.

1. Installera vald brandväggslösning på datorn med 2 nätverkskort. Se till så att nätverkskorten är anslutna korrekt. Gör den grundläggande konfigureringen (IP-inställningar, användarnamn etc.).
2. Se till så at klientdatorn är ansluten korrekt och fungerar.
3. Konfigurera klientdatorn så att den har Internetanslutning via er brandvägg.
4. Anslut till brandväggens grafiska (webb?)gränssnitt.
5. Vad innebär *Traffic shaping/QoS* ? Hur aktiverar man detta*?*
6. Blockera FTP-trafik, testa och dokumentera. Återställ/ta bort regeln sedan.
7. Blockera ALL trafik utom FTP, testa och visa. Återställ/ta bort regeln sedan.
8. Vad innebär Proxy? Hur aktiveras webb-proxyn? Vilka andra proxy-tjänster kan aktiveras?
9. Hur gör man för att blockera nätverksaccess under en viss tid på dygnet?
10. Vad finns det för övervakningsmöjligheter?
11. Har vald brandväggslösning stöd för VPN och vilken typ i så fall.
12. Vad innebär *stateful packet filtering*?