COMPUTERWORLD

Firewalls en forklaring for den (måske mere end) almindelige brugere.

Sikkerhed er fyldt med upræcise begreber, der bruges forskelligt. Denne artikkel forsøger at give et bud på hvordan det hænger sammen. Når du har læst den, er du mindst forvirret på en højere niveau. Artiklen er relativt teknisk.

Skrevet den **08. Feb 2009** af **bufferzone** I kategorien **Firewalls / Generelt** | ★★☆☆☆

Firewalls. En forklaring for (den måske ikke helt) almindelige brugere.

Ligegyldigt hvor man læser noget om computersikkerhed lyder rådet "du skal have en firewall". Det lyder jo enkelt nok, man så opdager men at der tilsyneladende er flere forskellige firewall's. Der tales om software og hardware firewall's om bastions firewall, om routere med indbyggede firewalls. Hvad skal man nu bruge?, giver de den samme sikkerhed? Nedenstående artikel er et bud på hvordan man kan forklare de forskellige typer, samt et bud på hvad du kan bruge de forskellige typer til. Du skal vide at emnet kan behandles på andre måder, og at især de forskellige fabrikanter er interesseret i at fremstille sagen, så lige netop deres produkt fremstår som en rigtig firewall, der giver god sikkerhed og er det rigtige valg.

Teknologi.
Personligt kan jeg bedst lide at kikke på teknologien bagved for at forklare hvordan de forskellige typer af firewalls virker. For at kunne dette, er vi først lige nødt til at kikke på, hvordan man normalt opdaler netværkskommunikation. Til dette anvender man OSI's reference model, der opdeler den proces data undergår når der kommunikeres fra bruger til bruger over et netværk. Du kan her se en grafisk præsentation af modellen samt en forklaring på hvad der sker i de enkelte lag
http://www2.rad.com/networks/1994/osi/layers.htm.

```
Lag 7 Applikations lager: Stiller forskellige services til rådighed for
applikationerne

Lag 6 Præsentations laget: Konvertere informationerne

Lag 5 Sessions laget: Håndtere forskellige problemer, der ikke har forbindelse
med selve kommunikationen

Lag 4 Transport laget: Håndtere kontrol kommunikationen fra punkt til punkt

Lag 3 Netværks laget: Håndtere routning af informationerne I netværket

Lag 2 Data Link laget: Håndtere fejlkontrol mellem forskellige maskiner på
netværket

Lag 1 Fysiske lag: Håndterer fysisk adgang til netværket.
```

Nu har vi fuldstændig styr på netværkskommunikation.

No-Shit-Sherlock, selvfølgelig har vi ikke det, for at kunne forstå hvordan en firewall virker i detaljer, er du selvfølgelig nødt til at læse lidt selv, men vi bruger nu ovenstående model til at forklare forskellene på de forskellige firewalltyper, og jeg skal nok give praktiske eksempler på hvad forskellene betyder i den virkelige verden.

Man kan dele firewalls op i to grundlæggende forskellige typer, efter hvor langt op i OSI modellen de arbejder. Den mest almindelige type er pakkefiltreringsrouteren der findes i stort set alle routere og switche der har firewall funktionalitet og så er der den professionelle "rigtige" firewall, kaldet en Applikations proxy, Applikations firewall eller en Applikations Gateway, Der er her tale om en meget avanceret firewall, der giver rigtig god sikkerhed og som normalt koster kassen.

Pakke filtrerings routeren.
Pakkefiltrering sker til og med lag 3 i OSI modellen og kan dermed kontroller IP header informationen. Source og destination adresser, hvilken service eller protokol der er tale om, men ikke selve dataindholdet. Traditionelle pakke filtreringsroutere betjener sig af statiske regelsæt der tillader (allow) eller afviser (deny) pakker baseret på ovenstående informationer. Pakkefiltreringsroutere betegnes ofte som den mindst sikre form for firewall, men den vil være rigeligt til de fleste private og små firmaer, hvis den kombineres med andre ting.

her er nogle eksempler på pakke filtrerings routere.
De fleste almindelige routere
Cisco Standard og extented routers (ikke med reflexive)
IPChains
det meste VPN hardware
Hvis der ikke reklameres med Stateful Inspection, så har boksen det ikke

Stateful Inspection firewall.
Her bør du faktisk læse min artikel Opbygning af firewall regler. Overvejelser med mere (http://www.eksperten.dk/artikler/554) der giver en bedre og mere nuanceret forklaring.

Stateful Inspection kaldes ofte for dynamisk pakket filtrering og er grundlæggende en pakket filtrerings router men ekstra intelligens og hukommelse. Hvor pakkefiltrering basere sine afgørelser på IP header informationer, inkorporere Stateful Inspection også kommunikationens kontekst og state i beslutningen. Selvom Stateful Inspection firewalls stadig kun bevæger sig op til lag 3 i OSI modellen opnår de faktisk en slags kontrol med de højrere lag ved at tracke kommunikations og applikations afledt state og ved at store og dynamisk opdatere disse informationer. Sagt på dansk er forskellen mellem pakkefiltrering og stateful inspection at pakke filtrering ansætter en portvagt, der kan læse adgangskortene for at se om folk må passere. Stateful inspection portvagten lærer også de enkelte ansatte at kende, samt deres gang i organisationen, og kan på den måde mere sikkert afgøre om nye personer må passere eller ej, baseret på oplysninger om hvordan "normal" kommunikation bevæger sig gennem firewallen.

Stateful and stateless are adjectives that describe whether a computer or computer program is designed to note and remember one or more preceding events in a given sequence of interactions with a user, another computer or program, a device, or other outside element. Stateful means the computer or program keeps track of the state of interaction, usually by setting values in a storage field designated for that purpose.

http://www.ssimail.com/Stateful.htm

her er nogle eksempler på stateful inspection firewalls
Cisco Firewall Freture set
Cisco Pix
Checkpoint Firewall-1
SonicWall

Linux Netfilter
BSD IPFilter og ipf
Netscreen

Applikations Proxyen.
En Applikations Proxy er et ret avanceret stykke software, der giver meget høj sikkerhed, og kan beskytte mod nogle ting pakkefiltrerings routeren aldrig kommer i nærheden af. Applikations Proxyen arbejder helt op på lag 7 i OSI modellen, og kan således kontrollere og filtrere hele datapakken inkl. Dataindholdet. Applikations Proxyen skal kende den kommunikation den skal kunne håndtere. Det betyder at firewallen skal indeholde proxy moduler til alle de forskelige protokoller den skal kunne håndtere. Normalt indeholder Applikatione Proxyen moduler til de mest almindelige former for kommunikation, d.v.s. web, mail, ftp. Applikations proxyen kan naturligvis håndtere den samme form for sikkerhed pakkefiltreringsrouteren med stateful inspection kan, men derudover kan den også kikke på dataindholdet. Det betyder at en applikations proxy kan sikre mod bufferoverflows, modificerede ICMP pakker, SQL Injections og andre former for angreb via modificeret og ondsindet dataindhold.
Den måde kommunikationen kører på "gennem" en applikations proxy er også anderledes en gennem en pakkefiltreringsrouter. Du har sikkert bemærket at ordet gennem er i citations tegn når jeg skriver om applikations proxyen, mens den ikke er det når jeg skriver om pakkefiltreringsrouteren. Dette skyldes at der faktisk ikke går kommunikation gennem en applikations proxy. Når en client har brug for at kontakte en service uden for det interne netværk, kontaktes firewallen. Den overtager så kommunikationen og kontakter den forespurgte service på klientens vegne. Det interne netværk kommunikerer kun med firewallen, Internettet kommunikerer kun med firewallen. Alt kommunikation mellem de to håndteres af firewallen. En Applikations proxy giver maksimal sikkerhed, især hvis den kombineres med DMZ (en artikel om dette er på vej), desværre koster den ofte kassen, så den er mest relevant for store virksomheder eller folk med særlige sikkerhedsbehov.

her er nogle eksempler på applikations proxy firewals:
Network Associate's Gauntlet Firewall
Symantec Enterprice Firewall (Raptor)
Microsoft ISA
BorderWare Firewall
WinGate
T.REX Open Source Firewall
Squid (oven på Netfilter)

Den personlige firewall Vs BAstions firewallen.
Jamen hvor ligger så den personlige firewall I dette spild, er det en pakkefiltreringsrouter eller hvordan???. Svaret på dette er at man her faktisk sammenligner æbler og pærer og at man ikke bør stille de to på mod hinanden, men snare bruge dem i kombination. Både pakkefiltreringsroueren og applikations proxyen kikker på netværkstrafikken ind og ud af det interne netværk. En software firewall kikker på de applikationer der kører på den enkelte computer og ønsker at tilgå nettet. Dette betyder at en software firewall kan opdage og melde når et stykke software på din computer ønsker at gå på nettet. Dette vil de andre firewalls ikke kunne opdage, hvis softwaren bare betjener sig af lovlig trafik

Hvad gør man så.
Du skal selvfølgelig have en firewall, og start bare med en personlig firewall, den vil give dig rimelig sikkerhed som privat. Hvis din router også har mulighed for at virke som pakkefiltrerings router, så brug også dette. Herefter kan du holde øje med markedet, teknologierne bliver mere udbrede og billigere og billigere. Applikations proxyen er i dag for de store organisationer, men om et par år er den allemandseje.

Denne artikel er lidt rå og ikke helt færdig endnu. Hvis du har spørgesml, kan du selvfølgelig altid stille dem her på eksperten, lige som du er velkommen til at kontakte mig med spørgsmål og kommentare på kim@bufferzone.dk

Kommentar af janbb d. 09. Feb 2004 | 1

meget 'teknisk' tilgang til emnet

Kommentar af nanoq d. 10. Feb 2004 | 2

En rigtig god artikel, der giver et udmærket indtryk af, hvad en Firewall egentlig er, og hvordan den kan arbejde. Jeg kunne godt ønske du sammenkoblede nogle af begreberne, med funktionaliteten på specifikke produkter (routere med simpel packetfiltering osv).

Kommentar af skwat d. 09. Feb 2004 | 3

A'okay!

Kommentar af pman d. 09. Oct 2004 | 4

Firewalls en forklaring for almindelige brugere... hehe okay jeg må være uvidende:o)

Kommentar af lun d. 19. Feb 2004 | 5

Lidt for teknisk til mit behov, men sikkert udmærket. Husk lige at på dansk er sammensatte ord ofte i et. Fx pakkefiltreringsrouter, Applikationsproxyen, filtreringsrouter, bastionsfirewall. vh den lille dansklærer :-)

Kommentar af krustytk d. 17. Feb 2005 | 6

Dejlig artikkel du beskriver tingene godt og grundigt.
Man får et godt billede af hva du prøver at fortælle, tror jeg ihvertfald ;) Jeg har fået en bedere opfattelse af firewall konceptet ihvertfald. :)

Kommentar af barbarbo d. 10. Feb 2004 | 7

Udgangspunktet er meget teknisk, men forklaret, så et almindeligt menneske forstår hvad forskellene på de enkelte firewall typer betyder, og hvad man skal vælge. Alle point værd

Kommentar af punnishment d. 22. Aug 2004 | 8

Ok artikel, men som du siger er den jo ikke færdig?
Derfor synes jeg godt du kunne indrage en vurdering af den intigrerede firewall i winXP. Er den rigelig, hvad kan den, ... ?

Kommentar af thomasso (nedlagt brugerprofil) (nedlagt brugerprofil) (nedlagt brugerprofil) d. 19. Mar 2005 | 9

God artikel!

Kommentar af root66 d. 12. Feb 2004 | 10

Godt skrevet. Kommer ud i de fleste hjørner. MEN, jeg ku' godt tænke mig lidt mere konkret, fx. effekten af en kombination af hhv. sw og hw-firewalls. Evt. med et par produktnavne: Hvor god er XP's, AVG's og lign. firewalls til at opfange "crack-ware" når man sammenligner dem.

Kommentar af serverservice d. 28. Oct 2004 | 11

-Hej Bufferzone , din artikel henvender sig ikke til den alm. bruger da den på et højt niveau, men derfor

synes jeg alligevel den er god for os netværksfolk som kender til firewalls og Osi.
Du bør måske ændre overskriften , f.x. Firewalls for den erfarne bruger?

Kommentar af smashlotus d. 23. Jun 2004 | 12

Firewalls - en forklaring for alm. brugere??!!! Næppe... Alt for teknisk. Nærmere en forklaring for professionelle it-administratorer!

Kommentar af rosenlunden d. 01. Nov 2004 | 13

Kommentar af bigshow d. 07. Oct 2004 | 14

Øj,øj,øj. Hvis dette er en forklaring til den alm bruger, af hvordan en Firewall virker, er min røv en vandflyver!) Vi er helt oppe og snakke ITA niveau, som der bliver gjort opmærksom på, andet steds. Men iøvrigt er det da godt, med folk der kan det der, med en "Brandmur".

Kommentar af frankieboy1 d. 10. Feb 2004 | 15

Meget informativ og lærerig. Er alle pointene værd.

Kommentar af dopey d. 15. Feb 2004 | 16

Muligvis en god artikel om emnet. Jeg havde håbet på at den var skrevet så "den almindelige bruger" kunne forstå lidt af det. Tro mig - der er næppe en fjerdedel at pc brugerne i Dk der bliver ret meget klogere af denne artikel. Vis nogen læser dette og har det i sig - kunne jeg gerne tænke mig at læse den samme artikel skrevet for "dopies".
Husk at mit ærinde ikke er at tale ned om artiklen - vi er blot mange der ikke forstår den.

Kommentar af sorenbs d. 24. Aug 2004 | 17

tak

Kommentar af forevernewbie d. 28. Aug 2004 | 18

Kommentar af ranglen d. 24. Aug 2004 | 19

Kommentar af fedora d. 30. Aug 2007 | 20

Jeg synes det er godt skrevet og forklar de forskellige aspekter. Jeg forstår folk som ikke har en teknisk forstand på Firewalls synes den er svær at forstå, men godt forsøg.

Kommentar af apromis d. 04. Nov 2004 | 21

Jeg kan ikke sige om den er god eller dårlig.. forstår nemlig hat af den :S

Kommentar af huset d. 21. Sep 2005 | 22

God artikel og alle 5 point værd!