Opbygning af firewall regler. Overvejelser med mere

Denne artikel er ikke for masserne, Den handler ikke om opsætning af personlige firewalls som XP's og Zonealarm. Hvis du overvejer at opsætte en firewall til beskyttelse af din net, ellere bare interessere dig for emnet, vil artiklen være noget for dig.

Skrevet den **04. Feb 2009** af **bufferzone** I kategorien **Firewalls / Generelt** | ★★★☆☆

Opbygning af firewall regler.

Alle firewall's kan fejlkonfigureres, eller konfigureres løsere end de behøver at være, og dermed give hackere og andre muligheder, der ikke burde være til stede. Faktisk er det relativt ofte man møder firewall's, der måske ikke er decideret fejlkonfigureret (selv om man også møder det) men som sagtens kan strammes op, uden det går ud over brugernes muligheder for, at anvende deres programmer og gå på nettet.
Generelt kan man sige, at jo længere en firewall har været i drift, jo flere løse ender vil der potentielt være. Du bør gennemse/overveje dit reglsæt jævnligt.

Nedenstående artikel er en gennemgang af de overvejelser og muligheder der bør gennemgås når man sætter sine firewall regler op, og igen før man gennemgår reglsættet igen.

Indgående og udgående reglsæt.
De fleste betragter en firewall som noget der skal beskytte deres computer eller netværk mod at nogen kan komme ind på det, hvorfor de indgående regler tillægges meget stor vægt. Se f.eks. Windows XP's indbyggede firewall. Den indeholder kun indgående filtrering og tillader alt udgående trafik. Firewallen i VISTA indeholder begge dele, men har som default kun den indgående filtrering konfigureret. Et skridt i den rigtige retning, men ikke nok. Dette er en kritisk fejl, der i mine øjne gør både XP's og Vista's firewalls anvendelighed begrænset. Firewallen give sikkerhed mod at vira og orme kommer ind på maskinen i første omgang, men smittes maskinen af andre kanaler (e-mail eller inficerede filer og dokumenter) vil din maskine kunne sprede både vira og orme uden begrænsning. Sikring mod hackere er også mere begrænset end hvis der havde været et fornuftigt udgående regelsæt.

Grunden til at udgående regler er mindst lige så vigtige som indgående skal findes i den måde hvorpå hackere og orme ofte arbejder. En sårbarhed i dit system udnyttes via et exploit til at få din maskine til at forbinde sig ud til hackerens maskine, hvorefter hackeren henter de nødvendige værktøjer til din maskine. Ofte vil hackeren kunne anvende Internet Explorer til at hente data og værktøjer med, den, eller tilsvarende browser, findes jo på de fleste systemer. Hvis hackeren "kun" har adgang til en kommando prompt (dvs. han kan skrive tekst kommandoer til/med din computer), vil han kunne anvende helt almindelige FTP kommandoer, og forbinde sig til sin egen FTP server. Det er med andre ord ikke hackeren der bryder ind, men ham der får din maskine til at bryde ud Hvis der havde været opstillet fornuftige udgående regler, kunne denne trafik måske have været stoppet i firewallen og angrebet afvist.

Lukke huller eller åbne huller.
Igen har vi fat i noget virkeligt grundlæggende. Skal man starte med at tillade alt så det er let for både brugerne og administratoren, og derefter lukke for de farlige huller? Eller skal man starte med at lukke alt, og derefter åbne for det absolut nødvendige? Microsoft har i årevis fulgt det første princip for at lette brugervenligheden, men der er ingen tvivl om, at det sikkerhedsmæssigt er langt bedst at starte med at lukke helt af og så kun åbne for det der positivt er nødvendigt og fornuftigt. Lav en positiv liste over hvad brugerne må, og tillad dette, i stedet for en negativ liste over hvad de ikke må.

Reglernes rækkefølge.
Den rækkefølge en firewall's regler listes i, er meget vigtig, her kan man lave både uhensigtsmæssigheder og deciderede fejl, hvis man ikke tænker sig godt om. Fejlene opstår særligt ofte når regler senere tilføjes eller der flyttes rundt på reglerne, sikkert fordi man ikke har så godt overblik over alle reglerne, som da man første gang skrev reglsættet.
Problemet opstår fordi trafikken behandles efter den FØRSTE regel der passer og dermed ikke nødvendigvis den bedste regel.
Grundlæggende findes to "skoler" du kan følge. Du bør altid placere de mest specifikke regler først og mindst specifikke regler sidst, Herefter kan du så vælge mellem at prioritere firewallens performance eller applikationernes ventetid. Hvis du placere de mest brugte regler først, vil du optimere regelsættet til firewallens performance hvis du placere regler der "betjener" de vigtigste applikationer først vil du optimere til applikationerne. Ofte kan du kombinere de to, idet det altid er afgørende vigtigt at kontrollere at man ikke har lavet et hul for sig selv ved at placere en mindre specifik regel foran en mere specifik.

Et relevant eksempel kunne f.eks. være at du har lavet en specifik regel der kun tillader din DNS server at tilgå den IP adresse hvorpå din eksterne DNS server ligger og kun på port 53. Senere opdager du så, at reglen om, at alle dine maskiner må tilgå alt på port 80, bruges hele tiden, hvorfor du flytter den op først i regelsættet. Du har nu lavet et hul i dit regelsæt, idet din DNS server nu kan tilgå alt på port 80 og det skal den selvfølgelig ikke, en DNS server skal ikke surfe på nettet, og hvis den gør det, er der noget alvorligt galt som f.eks. at en hacker har kontrol med den og har brugt browseren til at hente værktøjer op med.

Indgående regler.
Hvad vi er nødt til at tillade, afhænger meget af hvilken type firewall vi har. En pakke filtrerings router er ikke så intelligent som en stateful firewall, der igen ikke er så intelligent som en stateful inspection firewall. Jeg er derfor nødt til at opdele overvejelserne efter hvilken type firewall vi taler om.

Generelle overevejelser for alle typer.
Udover typen af firewall er der to områder vi skal kikke på, når vi overvejer den indgående trafik. Dels den trafik der kommer ude fra og skal ind til tjenester vi udbyder, f.eks. hente web sider fra vores web server, hente filer fra vores ftp server eller levere mails til vores mailserver. Og dels den trafik der skal ind gennem firewallen som svar på noget der er forespurgt indefra, f.eks. en bruger der ønsker at se en web side fra en fremmed webserver.

pakkefiltreringsrouteren.
Vi er nødt til at åbne for portene til de tjenester vi udbyder på vores net. Dvs. f.eks. port 80 til vores web server og port 25 til vores mailserver, MEN det er måske ikke nødvendigt generelt at åbne for alt indgående trafik på disse porte. Måske kan vi nøjes med at tillade trafik på port 80, der specifikt er til vores web server, så man ikke kan tilgå f.eks. mailserveren eller alle arbejdsstationerne på port 80. Samme forhold er gældende for de andre porte.
Når vi har indsnævret tilladelserne så man kun kan tilgå de systemer vi ønsker via den port vi ønsker, lad os så kikke på hvem vi vil tillade forbindelser fra.
F.eks. er der ingen grund til at tillade forbindelser der kommer fra interne IP adresser hvis de kommer udefra. Det lyder måske som om at den slags ikke burde kunne ske, men det gør det ofte. Disse forbindelser er enten spoofede IP adresser eller fejlkonfigureret NAT udstyr. Interne loop back IP adresser (127.0.0.1), ikke allokerede/reserverede IP adresser (se her hvilke der er reserverede http://www.iana.org/assignments/ipv4-address-space) samt IP adresser fra områder hvorfra der kommer meget skidt (se Internet Storm Center top 10 på http://isc.sans.org/top10.php) bør heller ikke tillades adgang udefra. Overvej altid om tilladelsen kan præciseres og dermed snævres ind. (ovennævnte adresser er et eksempel på hvad der bør forbydes, da det ville kræve mere konfiguration positivt at tillade de adresser der må komme ind). Antispoofing er det eneste sted i regelsættet hvor man fraviger princippet om at forbyde alt og tillade det nødvendige

Herefter er vi nødt til at sørge for at svarene på vores forespørgsler inde fra kan komme tilbage. Her løber vi så ind i det problem at en pakkefiltreringsrouter ikke kan holde state (fordansket fra det engelske "to maintain state", der betyder "holde styr på" sammenhængen mellem de enkelte ud- og indgående pakker,

samt holde styr på sammenhængen mellem forespørgsel og svar), hvorfor vi er nødt til at åbne alle såkaldte ephemeral ports, dvs. porte over 1023. Det er sådan at når en bruger f.eks. ønsker at åbne www.sans.org i hans browser, så sendes en forespørgsel på port 80 men et svar port på f.eks. 25.000 (svar porten vælges tilfældigt blandt portene større end 1023).

Stateful router/firewall.
De samme principper og overvejelser som vi brugte for pakkefiltreringsrouteren gælder også for en stateful router/firewall, men de porte der skal åbnes for at tillade svar på forespørgsler at komme tilbage, håndteres væsentligt mere intelligent, når vi bruger stateful filtrering. I stedet for at åbne alle porte over 1023, virker firewallen på den måde at alle forespørgsler noteres i en såkaldt state tabel. Når en pakke så forsøger at komme ind gennem firewallen, vil denne lave et opslag i sin state tabel for at se om denne pakke er et svar på en tidligere forespørgsel. Hvis firewallen positivt identificere pakken som tilhørende en tidligere forespørgsel vil den åbne den nødvendige port for denne ene pakke i det øjeblik den passere og derefter lukke porten igen. Dette er, alt andet lige, et meget mindre hul end det vi er nødt til at åbne i en pakkefiltreringsrouter.

Stateful Inspection Friewall.
Med stateful inspection bliver det igen lidt mere intelligent. En firewall der kun er stateful, bruger den information der står i pakke headeren til at se om der er tale om en pakke der hører til en anden pakke eller hører til et svar på en tidligere forespørgsel og det vil i de fleste tilfælde være nok til at afgøre tingene. Der er dog nogle protokoller hvor man er nødt til at kikke i dataindholdet for at se at der faktisk er tale om en pakke der hører til en tidligere afsendt forespørgsel. En sådan pakke vil med en stateful firewall blive droppet mens en stateful inspection firewall kan håndtere den og lukke den igennem.
ICMP protokollen bruges bl.a. til ping, men den bruges også (måske endda mest) til at give fejl meddelelser til midlertidige fejlsituationer på nettet. Hvis en bruger på dit net f.eks. ønsker at åbne www.giac.org i sin browser, og denne side er nede, vil den sidste router på vejen ikke kunne aflevere forespørgslen til den server der indeholder web siden. I stedet vil routeren sende en såkaldt ICMP host unreachable pakke tilbage til brugeren på dit net. Når denne pakke rammer din firewall vil en stateful firewall se en pakke der kommer fra en router som den selvfølgelig ikke kan finde nogen forespørgsel der passer til, da brugeren jo forespurgte en web side. Er firewallen en statefil inspection firewall, vil denne kende ICMP protokollen og vide at den skal kikke i pakkens dataindhold for at se hvilken kommunikation pakker faktisk er svar på. ICMP pakken vil blive lukket ind, og brugeren vil få at vide at serveren er nede. Havde firewallen kun været stateful, ville forbindelsen være forblevet åben og browseren ville have ventet på svar indtil forbindelsen timede ud.

Udgående regler.
De udgående regler er som sagt er relativt overset område, og der er mange som antager den holdning, at alt skal være tilladt indefra og ud, det er jo de interne brugere der sidder på indersiden af nettet, så det er jo ikke farligt, at de kan gå ud med alt og det giver alt for mange problemer at starte med at lukke alt.
Mit råd er igen at start med at luk for alt, hvorefter der åbnes for det der er nødvendigt. Hvis dine brugere skal kunne browse Internettet, er det f.eks. nødvendigt at åbne for port 80. Start med at åbne for port 80, men tillad kun de klientmaskiners IP adresser du faktisk bruger på din net at kommunikere ud gennem porten. Der er f.eks. ingen grund til at din fil og print server kan gå på nettet, hvorfor skulle den dog det? Din mail server har heller ikke brug for at kunne gå på nettet via port 80 og hvis den gør det, er der sandsynligvis noget galt. Port 53 bruges til navneopslag og opløsning mellem www navne og IP adresser. Det sikreste er at have en intern DNS server, som klienterne kan foretage navne (DNS) opslag på. Denne DNS server, og KUN DEN, skal så have lov til at kommunikere med en extern DNS server via TCP og UDP på port 53 og det er vigtigt at du kun tillader kommunikation fra din DNS servers IP adresse til den externe DNS servers IP adresse på port 35 (TCP og UDP).
Hvis du har et lille hjemmenetværk uden DNS server, bør du sætte reglerne op således at kun dine klienters IP adresser kan kommunikere med den primære og den sekundere DNS servers IP adresser på port 53 (TCP og UDP) og ikke andet

Tænk dig om.

Selv den dyreste firewall giver ingen sikkerhed, hvis den ikke er ordentligt konfigureret og hvis du ikke tænker dig om, risikere du at lave regler, der giver muligheder, der ikke behøver at være til stede og som kan udnyttes af den dygtige hacker.

1. Start altid med alt lukket og slukket.

2. Placer de mest specifikke regler før de mindre specifikke regler, og tænk dig grundigt om før du ændrer i rækkefølgen.

3. Giv kun udgangstilladelse til de IP adresser på dit net der absolut skal bruge tilladelsen, og kun med de porte der er behov for.

4. Giv kun indgangstilladelse til IP adresser udefra på de nødvendige porte, der bør og skal ind, filtrer resten fra.

5. Hvis du kan begrænse tilladelsen til bestemte destinations IP adresser udgående, bestemte source IP adresser indgående, på bestemte porte, med TCP eller UDP og ikke andet, så gør det.

Følger du ovenstående principper sikre du dig dels, at kun det mest nødvendige kommer ind, samt at du er en god Internetnabo der ikke udsender spoofede pakker og andet.

Skulle du have spørgsmål, kommentarer eller rettelsen (herunder især stavefejl) er du velkommen til at kontakte mig på kim@bufferzone.dk, ligesom jeg ofte er at finde på Eksperten. Jeg hjælper selvfølgelig også gerne med de forskellige værktøjer. Undlad venligst at stille spørgsmål i kommentarerne, dem kan jeg jo ikke svare på.

Kommentar af nogetfx d. 09. Feb 2005 | 1

Kommentar af phatlasse (nedlagt brugerprofil) d. 22. Dec 2004 | 2

lækker artikel, der gør at man får en grundlæggende forståelse for hvordan man skal tænke, ved opsætning af firewall.

Kommentar af xyborx d. 23. Dec 2004 | 3

Ikke så meget nyt for mig, udover forskellen på stateful og stateful inspection. Jeg troede det var synonymer. Absolut værd at læse for enhver der skal sætte en firewall op.

Kommentar af dinky d. 25. Jan 2007 | 4

Kommentar af zerocrash d. 07. Jun 2006 | 5

Meget god artikel om sikkerhed. For mig gav den nyt omkring forskellen på statefull og statefull inspection firewalls...

Kommentar af hmann d. 22. Dec 2004 | 6

Der blev jeg faktisk en del klogere på de forskellige typer firewalls. Dejligt enkelt og forståeligt! Thumbs up! /HMann

Kommentar af smasher1000 d. 22. Nov 2008 | 7

TAK!! SÅ fattede jeg endelig forskellen på stateless og statefull firewalls.

Kommentar af keodk d. 03. Jan 2005 | 8

Kommentar af janpo d. 21. Apr 2007 | 9

Fin artikel. Hvert et point værd.
Et par små skønhedspletter alt afhængig af hvem man er, men kanon gode regler for folk med hjemme netværk.

Kommentar af hansilansi d. 07. May 2005 | 10

God og meget godt beskrevet. Der er gode detaljer, og man forstår den nemt! Virkerlig ALLE 5 point værd, alle skulle læse den, og blive klogere;)

Kommentar af sorenbs d. 22. Dec 2004 | 11

Værd at læse:)

Kommentar af m-smith d. 21. Dec 2004 | 12

Flot arbejde

Kommentar af freehelp d. 22. Dec 2004 | 13

Ikke noget nyt for mit vedkommen - men alt i alt en rigtig god artikel og point værd!

Kommentar af andr3as d. 30. Dec 2004 | 14

Kommentar af andber d. 07. Jan 2005 | 15

Kommentar af kazx d. 25. Jun 2007 | 16