Syddansk Universitet

DM830 - Netværkssikkerhed

Imada - Institut for matematik og datalogi

Forår 2012 - Firewalls

Forfatter:
Daniel Fentz Johansen
Alexei Mihalchuk

Underviser:
Prof. Joan
Boyar

Indhold

1 Indledning

Formålet med denne rapport, er at give et overblik over emnet firewalls i faget netværkssikkerhed. Rapporten kan bruges som en hjælp, da den dækker de vigtigste emner.

2 Hvad er en firewall?

En firewall er et stykke software eller netværksudstyr som beskytter et netværk fra trusler udefra. Firewall blev oprindelig brugt om vægge i huse, som blev brugt til at afskærme afdelinger fra brand i andre dele i huset. Deraf navnet firewall, eller brandmur på dansk.

2.1 Første firewall

Firewalls som vi kender dem i dag, begyndte at dukke op sent i 1980'erne. De var af typen packet filtering, og var implementeret som software i routere. I starten af 1990'erne gik det rigtig stærkt, og både stateful firewalls og application level firewalls kom frem.

3 Behovet for en firewall

Er det overhovedet nødvendigt med en firewall? Hvis vi kigger på udviklingen for virksomheder og offentlige institutioner de sidste årti.

- Internet forbindelser er blevet et must for at virksomheden kan fungere.
- Alle computere i virksomheden er koblet sammen.
- I virksomheden er der mindst en server til at administrere ting som ordre, økonomi, osv.

Hvordan beskytter man alle computere i en virksomhed? En løsning på dette ville være at installere en firewall, samt et antivirusprogram, på alle virksomhedens computere. Dette ville imidlertid ikke være en særlig effektiv løsning, da en ændring i firmaets sikkerhedspolitik ville betyde, at en it-ansvarlig skulle rundt på samtlige computere i virksomheden og omkonfigurere dem. Derudover, så kører virksomheder oftest med flere forskellige platforme of styresystemer, hvilket komplicer konfigurationen.

4 Mål for en firewall

Når man desiger en firewall er der visse mål man skal have for øje. Der er 3 hovedpunkter:

- Alt trafik udefra og ind, og omvendt, skal fysisk igennem firewallen. Dette sikrer at man ikke kan omgå firewallen.
- Det er kun trafik som er tilladt via firmaets sikkerhedspolitik som får lov til at komme igennem firewallen.

- Firewallen skal være immun overfor angreb. Ofte er firewallen baseret på et ekstra sikret operativsystem.

For at firewalls kan opnå disse mål, benytter de et sæt af teknikker.

- Service Control: Hvilken slags trafik er tilladt? Filtrering kan ske på baggrund af IP-adresser eller mere avanceret teknikker såsom proxyer.
- Direction Control: I hvilken retning er denne trafik tilladt? Noget trafik er måske kun tilladt ud af huset, mens andet også er tilladt ind. Det kan være det er tilladt at forbinde til en FTP server ud af huset. Men at udefra kommende ikke kan forbinde til en FTP server som står inde i huset.
- User Control: Hvilke brugere har ret til en bestemt tjeneste? Et eksempel kunne være, at det kun var ansatte i it.afdelingen som havde adgang til firmaets udviklingsserver. Dette kunne sikres ved at kigge på de IP-adresser, der prøver at forbinde til udviklingsserveren og kun tillade de, som matcher de ansattes i afdelingen. Mere avanceret kontrol på baggrund af hvilken bruger der er logget ind på computeren findes også.
- Behavior Control: Hvordan er det forventet at en tjeneste opfører sig? Hvordan forventer man foreksempel at en FTP client opfører sig når man forbinder ud af huset? Dette kan bruges til at opdage uønsket adfærd i programmer man har tillid til. Man kan måske opdage, om ondsindet software prøver at udgive sig for at være et program som virksomheden har tillid til.

Det kan hurtig lyde som om at firewallen kan løse de fleste udfordringer en virksomhed står overfor med hensyn til sikkerhed. Men det er vigtigt at kende de begrænsninger en firewall har.

- En firewall kan ikke beskytte mod angreb som omgår, eller på anden måde kommer forbi firewallen.
- En firewall kan ikke beskytte mod interne trusler. Det kan være en sur medarbejder, der samarbejder med en hacker.
- Et dårligt sikret trådløst netværk er også en udfordring, da netværket oftest ligger internt - efter firewallen.
- Bærbart udstyr kan blive inficeret uden for virksomheden, og dermed bære smitten med ind i huset og sprede sig.
- Endelig er der mange former for ondsindet software som kan sprede sig gennem programmer og tjenester man har tillid til - email, webbrowser, osv.

5 Typer af firewall

Der findes forskellige slags af firewalls. Vi har valgt at dele dem op i 3 typer.

1. Packet Filtering: Filtrerer pakker udfra header-information.

2. Stateful Packet Inspection: Bygger på samme princip som Packet Filtering, men ser dog pakkerne i en sammenhæng.
3. Application Level: Opererer på et højere lag i OSI modellen. Fungrerer som en proxy mellem tjenester.

6 Packet Filtering Firewall

Packet Filtering Firewall er en firewall, som filtrerer indkommende og udgående data ved at inspicere netværkspakker. Baseret på et sæt regler, samt information indeholdt i netværkspakken, vælger en Packet Filtering Firewall enten at sende pakken videre eller smide pakken væk.

6.1 Filtrering af netværkspakker

For at kunne filtrere netværkspakker, aflæser en Packet Filtering Firewall information gemt i netværkspakken. Når en pakke bliver konstrueret, bliver der tilføjet header-information til pakken for hvert lag i OSI modellen, som pakken skal igennem.

For eksempel indeholder en pakke en IP-header, som beskriver IP-relateret information. Det omfatter blandt andet afsenderes IP-adresse, modtagerens IP-adresse, hvilken protokol pakken anvender (fx TCP), osv.

Baseret på denne information, matcher firewallen pakken med et sæt foruddefinerede regler. Hvis en netværkspakke matcher en regel, så kan firewallen enten sende pakken videre eller smide den væk, alt efter hvad der står i reglen. Hvis en pakke ikke matcher nogen regler, så bruges en generel politik til at diktere om en pakke skal sendes videre eller ej – for eksempel, så kan alle pakker, der ikke er eksplicit tilladte, kasseres.

6.2 Fordele og ulemper

De største fordele ved en Packet Filtering Firewall er, at den har et simpelt design, er diskret over for brugere og har næsten ingen overhead. Til gengæld har en Packet Filtering Firewall nogle begrænsninger, som gør denne type af firewall mindre hensigtsmæssig, hvis sikkerheden er første prioritet.

6.2.1 Angreb på tjenester

Hvis det skal være tilladt at tilgå en tjeneste udefra – igennem firewallen – er man tvunget til at tillade alle pakker sendt til tjenesten igennem. Da pakkefiltreringen ikke forgår i de højere lag i OSI modellen, bliver man nødt til at videresende alle pakker rettet mod tjenesten.

Hvis tjenesten indeholder fejl eller sikkerhedsbrister, så kan en ondsindet person uhindret konstruere og sende pakker af sted, som påvirker tjenesten negativt.

6.2.2 Begrænset logføring

Logføringen i en Packet Filtering Firewall er ret begrænset, da firewallen ikke har mulighed for at associere en pakke med meget andet end afsenderes IP-adresse. Dermed kan firewallen hverken genkende eller logføre, hvilke brugere

der er på netværket, og ved hvilken arbejdsstation de arbejder. Firewallen kan derfor hellere ikke genkende, om en ondsindet person forsøger at få adgang til systemet. Af samme grund kan denne type af firewall ikke autenticitere brugere.

6.3 Angreb på Packet Filtering Firewall

Udover de nævnte begrænsninger, så findes der angreb rettet direkte mod den måde, som en Packet Filtering Firewall og de underliggende protokoller arbejder på.

6.3.1 IP Address Spoofing

En firewall bruges til at skærme et internt netværk af computere fra resten af Internettet. Da der som udgangspunkt er tillid til de interne computere, bliver firewallen sat til at være mindre restriktiv over for dem.

IP Address Spoofing kan hjælpe en ondsindet person til at trænge ind i netværket. Personen skal konstruere en pakke, hvor afsenderens IP-adresse bliver sat til det samme som en af de interne maskiner.

Da en Packet Filtering Firewall bruger regelbaseret filtrering, så vil en pakke med en intern IP-adresse bliver tilladt. Den ondsindede person har nu adgang til computeren, og kan sende samme kommandoer, som godkendte brugerne ind for netværket.

For at løse problemet, så skal alle netværkspakker med interne IP-adresser stamme fra fra interne computere. Hvis en pakke kommer udefra, men indeholder en intern IP-adresse, så skal pakken kasseres.

6.3.2 Source Routing Attack

Når en netværkspakke bliver afsendt, kan pakken indeholde ruteinformation. Denne ruteinformation bruges til at optimere ruten, som pakken tager igennem Internettet, fx ved at specificere den hurtigste netværksforbindelse mellem afsender og modtager.

En ondsindet person kan bruge denne funktionalitet til at tvinge en pakke til at tage en rute igennem en specifik computer på det interne netværk. For eksempel, ved at sende pakker med Source Routing, kan en ondsindet person kortlægge dele af netværket eller få pakken til at se ud komme fra en intern netværk.

Løsning på problemet er, at ignorere alle netværkspakker der anvender Source Routing.

6.3.3 Tiny Fragment Attack

Når en Packet Filtering Firewall modtager en netværkspakke, skal den tjekke fel-terne i pakkens header. Hvis dele af header-informationen mangler, så kan en pakke fejlagtigt bliver godkendt, da pakken ikke vil matche nogen regler.

Dette problem kan give en ondsindet person mulighed for at omgå firewallen. Ved at bruge IP fragmentering, hvilket tillader, at en netværkspakke bliver delt op i fragmenter, kan personen konstruere en pakkefragment, som fx ikke indeholder en TCP-header.

Når firewallen ikke kan matche pakkefragmentet, kan pakken blive fejlagtigt tilladt. Det angreb kan forhindres ved at fastsætte et minimumsstørrelse for et pakkefragment.

7 Stateful Inspection Firewall

Stateful Inspection Firewall inspicerer også pakker, nøjagtig ligesom Packet Filtering, oven i bliver pakkerne også betragtet i en større sammenhæng. Nemlig om pakken er del af en ny forbindelse, eller en nuværende allerede etableret hukommelse. Dette giver yderligere muligheder for at konfigurere firewallen til at godkende forskellige mønstre som forskellige tjenester benytter.

8 Application Level Firewall

En Application Level Firewall giver den bedste beskyttelse, på bekostning af hastigheden. I forhold til de to forrige typer af firewalls, arbejder en Application Level Firewall i det højeste lag af OSI modellen. Det betyder, at firewallen har kendskab til de programmer som brugeren anvender.

En Application Level Firewall består oftest af to proxys, hvorimellem pakkerne bliver analyseret. Når en Application Level Firewall skal analysere en pakke, bliver pakkens header-information inspiceret - ligesom man gør ved pakkefiltrering. Men til forskel fra pakkefiltrering, så bliver selve dataet også undersøgt.

For eksempel kan en Application Level Firewall skanne pakker for virus. Derudover, så kan firewallen analysere pakken for gængse angrebsmønstre for programmet, eller forhindre specifikke pakker fra specifikke brugere.

Derudover, så understøtter en Application Level Firewall avanceret logføring og brugerkontrol.

9 Firewall Basing

Hvor har virksomheden tænkt sig at placere firewallen? En firewall kan installeres på en computer som et stykke software, men kan også være implementeret i en router, eller en speciel firewallboks man kan slutte til netværket.

9.1 Bastion host

En bastion host er en ekstra sikret computer, som kører en firewall. Ofte er disse computere speciel bygget til kun at køre firewallen. En bastion host har ofte en central rolle i firmaets netværk, og udgør en stærk barriere for eventuelle indtrængende.

9.2 Host baseret firewall

En host baseret firewall, er et begreb som bruges om en firewall som kører lokalt på en pc. Begrebet anvendes ofte for servere, hvor firewallen er installeret på de forskellige servere som firmaet huser. Dette ses som en modsætning til bastion host, hvor firewallen er placeret et centralt sted.

9.3 Personlig firewall

En personlig firewall, er et stykke software som er installeret på en pc. En personlig firewall adskiller sig fra en host baseret firewall, i det at den ofte ønsker at tilpasse sikkerheden løbende. Dette sker, som de fleste nok kender det, ved hjælp at pop-op meddelelser, hvor man skal tage stilling til om et konkret program skal have adgang eller blokeres.

Dette gør, at den enkelte bruger er ansvarlig for at konfigurere firewallen, modsat bastion host og host baseret firewalls, som bliver konfigureret af en it-ansvarlig, og kun ændret hvis firmaets sikkerhedspolitik bliver ændret.

10 Konklusion

Rapporten indeholder en overordnet beskrivelse af firewalls, samt de principper de bygger på. Der er også blevet givet en kort beskrivelse af de forskellige typer af firewalls. Med fokus i en Packet Filtering Firewall, er der blevet beskrevet, hvilke sikkerhedsmæssige problemer man kan støde på, samt hvilke angreb der kan bliver brugt mod firewallen.

Konklusionen er, at det er vigtigt for en virksomhed at have en firewall kørende. Men en korrekt konfigurationen af en firewall er ligeså vigtigt, da dette vil forhindre de fleste angreb.