Engineer

Brandvägg

regeluppsättningen som avgör vilken trafik som släpps igenom

Vad det är

En brandvägg är ett filter på en nätverksväg som jämför varje paket eller varje anslutning med en lista med regler och sedan släpper igenom trafiken, kastar den eller svarar med en vägran. Den kan vara programvara på den maskin den skyddar, en separat apparat mellan två nät eller en tjänst som en molnleverantör kör framför en virtuell maskin. Linuxadministratörer säger ofta paketfilter om samma sak, och molnleverantörer säljer brandväggar under namn som säkerhetsgrupp. I praktiken kommer brandväggar ofta i två lager: ett hos leverantören och ett på värddatorn.

Vägledningen från NIST i ämnet, SP 800-41 Rev. 1 från september 2009, sorterar dem efter hur mycket av trafiken de läser. Ett paketfilter tittar på adresser, protokoll och portnummer, ett paket i taget. En tillståndskänslig brandvägg minns dessutom anslutningar, så svaret på en begäran som servern själv gjorde släpps in utan en egen regel. En gateway med applikationsproxy avslutar anslutningen och läser protokollet inuti den. En värdbaserad brandvägg körs på den server eller bärbara dator som den vaktar och vet vilket program som äger en socket.

På en Linuxserver sker filtreringen i kärnans ramverk netfilter. nftables, som finns sedan kärnversion 3.13, ersätter de äldre verktygen i iptables, och gränssnitt som ufw skriver reglerna åt den som hellre anger en avsikt än bygger kedjor. Oavsett vad som skriver reglerna är modellen densamma: en ordnad lista som läses uppifrån, där den första regel som matchar avgör.

En brandvägg förväxlas ofta med närliggande verktyg. En brandvägg för webbapplikationer läser HTTP-förfrågningar och blockerar attackmönster i dem; en nätverksbrandvägg tittar aldrig så djupt. Ett verktyg som spärrar inkräktare läser loggar och lägger till tillfälliga regler mot adresser som beter sig illa, vilket

betyder att det förutsätter en brandvägg under sig. Ett VPN avgör vem som över huvud taget finns på nätet. Vart och ett av dem svarar på en annan fråga, och inget av dem ersätter den enkla regellistan.

Använd begreppet i ett beslut

Använd ”Vad är en brandvägg?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Konton, lösenord och behörigheter ordnade så att alla har exakt den åtkomst deras arbete kräver, och de som slutar förlorar den samma dag.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Skrev 1 000 RBAC-regler som säkrar Linux-servrar — 1,000 åtkomstregler, skrivna för att täppa till en säkerhetslucka

Skrev 1 000 RBAC-regler som säkrar Linux-servrar Hör av er →

Varför det spelar roll

Varje tjänst som lyssnar på en publik adress är en dörr, och brandväggen är förteckningen över vilka dörrar som finns. Att sätta upp den kräver ett beslut i tre delar: var brandväggen ska ligga, vad den tillåter som standard och vem som får ändra den.

En brandvägg hos leverantören stoppar trafiken innan den når maskinen, fortsätter att fungera om någon får root på värddatorn och kostar servern ingen processortid. Dess regler bor i en konsol eller ett API, utanför serverns egen konfiguration, så de glider isär från den om de inte skrivs som kod. En brandvägg på värddatorn följer med maskinen, kan hastighetsbegränsa en enskild port och kan testas från maskinen själv, men ett kapat root-konto kan skriva om den, och det kan även programvara som hanterar sina egna regler. Att köra båda är vanligt och förnuftigt, till priset av att två listor måste hållas i takt: varje port som öppnas eller stängs är en ändring på två ställen.

Standardläget är den andra delen. NIST rekommenderar att all trafik som inte uttryckligen är tillåten nekas, och för inkommande trafik håller nästan alla med. Det är vid filtrering av utgående trafik som avvägningen märks: den begränsar vad en kapad tjänst kan nå, och den stoppar paketuppdateringar, förnyelse av certifikat och övervakning tills varje destination har fått sin regel.

Den tredje delen är ägarskapet. En brandvägg som nekar som standard är bara så korrekt som den lista med portar som någon har deklarerat, så det användbara dokumentet är just den deklarerade listan, förvarad i versionshantering och kontrollerad mot de regler som faktiskt är aktiva. Programvaran är gratis i varje

vanlig Linuxdistribution; det som kostar är den uppmärksamhet som krävs för att hålla deklarationen sann. Och en brandvägg är en andra försvarslinje. En tjänst som är bunden till loopback-adressen går inte att nå utifrån, vad reglerna än säger, och det är en starkare garanti än en nekande regel framför en tjänst som lyssnar överallt.

Så ser det ut i praktiken

Brandväggen väcker här tre frågor: hur den kontrolleras, när den skapas och vad som kan ta sig runt den.

På en värddator låg en hastighetsbegränsning för SSH-porten i regellistan i ett år utan att ett enda paket nådde fram till den, eftersom en bredare tillåtande regel ovanför den matchade först. Statusverktygen listade begränsningen hela året, och de hade rätt att göra det: den fanns. Kontrollerna skrevs om för att läsa regelns position i stället för dess förekomst: de jämför nu ordningen i den numrerade regellistan, och i den kedja som kärnan faktiskt filtrerar med, mot det som var avsikten. Varje port får en regel och varje regel anger ett protokoll; SSH är hastighetsbegränsad och har ingen separat tillåtande regel. De fem publika portarna deklareras tillsammans och kontrolleras som en helhet, så en öppen port som deklarationen utelämnar gör kontrollen röd, och säkerhetsrapporten listar reglerna i den ordning som paketen möter dem, med en anvisning om hur den ordningen ska läsas.

Den första servern byggdes för hand och fick sin brandvägg först senare, vilket lämnade ett fönster då en ny maskin var nåbar från internet. För en andra server hos en annan leverantör skapas brandväggen av en egen play före maskinen, så den nya maskinen möter internet med sina regler redan på plats. Den leverantören kopplar brandväggar till maskiner med taggar, så taggarna skapas först: en regel som riktar sig mot en tagg kräver att taggen finns. Varje leverantörs brandvägg skrivs direkt mot leverantörens REST-API med en enkel HTTP-task. Den tasken gör ingenting vid en torrkörning, så ändringar provkörs i stället på brandväggens play, eftersom en brandvägg hos leverantören inte kostar något att skapa och går att ta bort igen.

Den tredje gäller containrar. Docker skriver in egna poster i kärnans paketfilter, och en port som Docker publicerar för en container matchas före allt som värddatorns härdningsroll har lagt dit, så en container kan vara nåbar utifrån vad brandväggen än har instruerats att göra. Den här plattformens containrar körs

under systemd genom Podman och Quadlet, delar värddatorns nätverk och publicerar inga portar, så det finns ingen containerport som något kan använda för att ta sig runt reglerna.

Var det går fel

En regel syns i statusutdatan men slår aldrig till. Regler utvärderas i ordning och den första träffen vinner, så en bred tillåtande regel som ligger ovanför en snävare begränsning eller nekande regel skuggar den helt. Listningen visar fortfarande båda. Läs reglerna som kärnan läser dem, numrerade och i ordning, lägg specifika regler ovanför allmänna och testa från en maskin utanför:

```
ufw status numbered
nft list ruleset
```

En container svarar på en port som brandväggen nekar. Docker publicerar portar genom att styra om trafiken i kärnans NAT-tabell, innan den når de kedjor som ufw filtrerar, och Dockers egen dokumentation säger att det i praktiken innebär att brandväggens konfiguration ignoreras. Publicera bara till loopback-adressen, sätt en brandvägg hos leverantören framför, eller kör containrar utan publicerade portar som beskrivs ovan.

IPv4 är låst medan IPv6 står vidöppet. De två adressfamiljerna har separata regeluppsättningar i iptables, och ufw skriver regler för IPv6 bara när IPv6 är påslaget i dess fil med standardinställningar. En värddator med en publik IPv6-adress och en regeluppsättning för enbart IPv4 är exponerad på varje port som den lyssnar på. Använd en tabell i nftables av familjen `inet`, som ser båda, eller granska båda listningarna, och skanna värddatorns IPv6-adress utifrån.

SSH-sessionen fryser i samma ögonblick som brandväggen slås på. Nekandet som standard blev aktivt före regeln för SSH, eller så flyttades SSH-daemonen till en annan port medan regeln fortfarande anger 22. Lägg till regeln för SSH först, håll leverantörens konsol öppen i ett annat fönster och schemalägg en automatisk återställning några minuter fram i tiden, som avbryts så snart en ny session kommer in.

En regel öppnar mer än författaren avsåg. I ufw öppnar en regel som anger en port utan protokoll den för både TCP och UDP. Ange protokollet i varje regel, och deklarera den förväntade ytan som en helhet, så att allt extra fäller en kontroll i

stället för att vänta på en revision.

Läs mer

- Firewall — definitionerna som publikationer från NIST använder, var och en länkad till sitt källdokument.
- SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy — brandväggstyper, en policy som nekar som standard och hantering av regler, från NIST.
- ufw(8) — brandväggsgränssnittet i Ubuntu, bl.a. regelordningen och regeln `limit`.
- nftables wiki — dokumentationen från projektet netfilter för det ramverk som ersätter iptables.
- Packet filtering and firewalls — Dockers egen redogörelse för hur publicerade portar passerar förbi en värddators regler.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är en brandvägg?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/firewall/