Brandväggs-lösningar

Minimera komplexiteten

Nätverkstjä*nster*
- Finns kända och okända

Förenkla
- Ta bort alla onödiga tjänster
- Ta bort onödig trafik
- Ta bort onödiga hostar

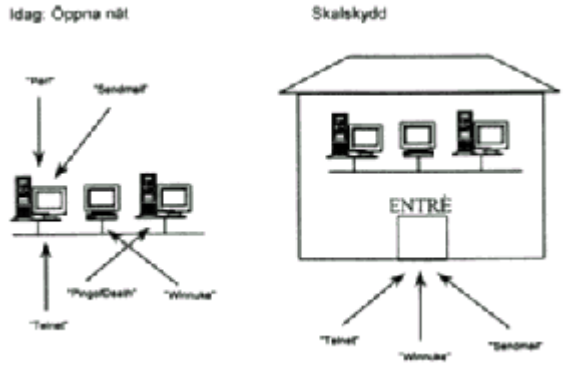
Spärra trafik
- Spärra hellre för mycket än för lite

Nätverkstjänster:
Alla nätverkstjänster innehåller både kända och okända säkerhetsrisker. Med varje tjänst finns det en risk att det någon gång i framtiden uppdagas ett säkerhetsproblem.

Förenkla:
Ta bort alla onödiga tjänster. "Del spelar ingen roll om det finns säkerhetsrisker i en tjänst så länge den inte körs".

Spärra trafik:
Det är bättre att spärra för mycket trafik än för lite. Spärrar vi för mycket kommer användarna att klaga, om vi spärrar för lite får vi inga samtal.

Skalskydd för företag



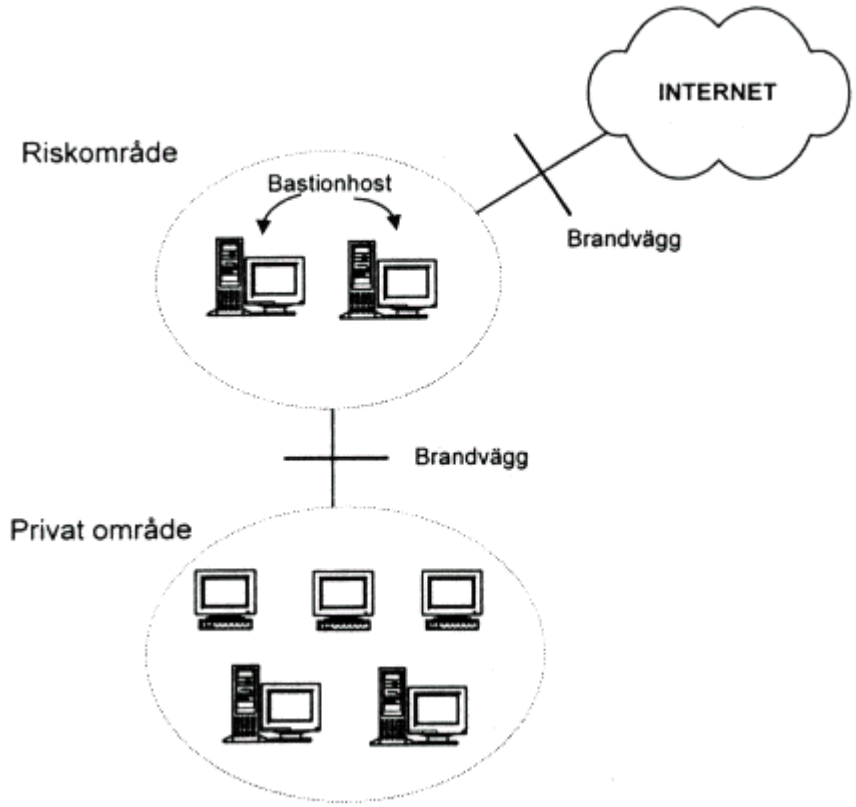
Öppna nät
- Ingen kontroll
- Inga filter

Skalskydd
- Filter
- Loggning
- Autenticering

Öppna nät:
Ingen kontroll eller loggning
Inga filter som stoppar viss typ av trafik till visa hostar

Skalskydd:
Filter som stoppar eller tillåter viss typ av trafik
Filter som stoppar eller tillåter trafik till hostar
Loggning av tillåten trafik och icke tillåten trafik
Autentusering av personer eller hostar

Terminologi



Privet område:
På det privata området finns de flesta av företagels datorer. Dessa skall inte var åtkomliga från något annat område, vilket leder till att vi inte behöver säkra upp dem för yttre hot. På detta område finns också företagets interna servrar.

Riskområde:
På riskområdet finns datorer routrar och tjänster som kommer att vara åtkomliga för attacker.

På riskområdet:
- Får bara datorer av strategisk betydelse finnas
- Kontinuerlig loggning som skall på ett säkert sätt föras in till det privata området.
- Larm skall gå om attack detekteras

Bastionhost:
Är en dator som är åtkomlig för attacker.
Skall:
- Vara ansvarsfördelande
- Ständigt uppdateras med nya programvaror
- Ge larm vid incidenter och utföra loggning
- Regelbundet granskas

Brandvagg:
Utgör skydd mellan områden

Tre typer av brandväggar

Paketfiltrering

Denna typen av brandvägg gör ingenting med själva paketet. Utan tittar endast i IP fälten och tar beslut.

TCP-koppel

Arbetar med sessioner/sockets mot brandväggen. Detta kräver att det finns installerade klientprogramvaror på alla datorer som vill komma igenom brandväggen.

Applikationsnivå

Jobbar på alla nivåer i OSI-modellen och kan således ta beslut rörande nästan vad som helst. Denna typen är den mest avancerade.

Paketfiltrering

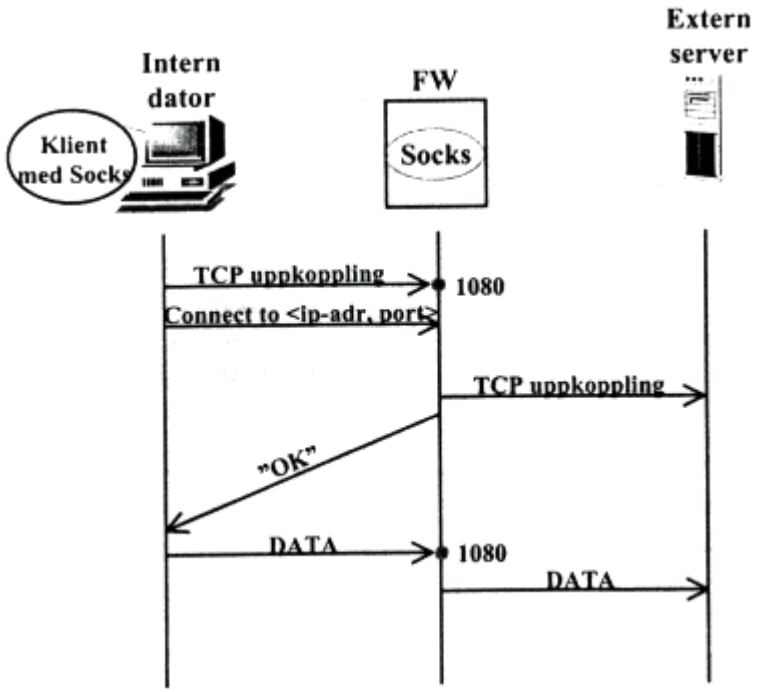
Snabba filtreringsbeslut
Kräver god kunskap om protokollen

Två typer:
- Utan tillståndsberoende filtrering
- Med tillståndsberoende filtrering

Utan tillståndsberoende filtrering;
Filtret måste öppnas för trafik in och ut, protokoll för protokoll.

Med tillståndsberoende filtrering:
Inkommande trafik tillåts endast efter utgående trafik.
Förenklar konfigurationen. Brandväggsroutern håller reda på trafiken.

TCP-koppel nivå

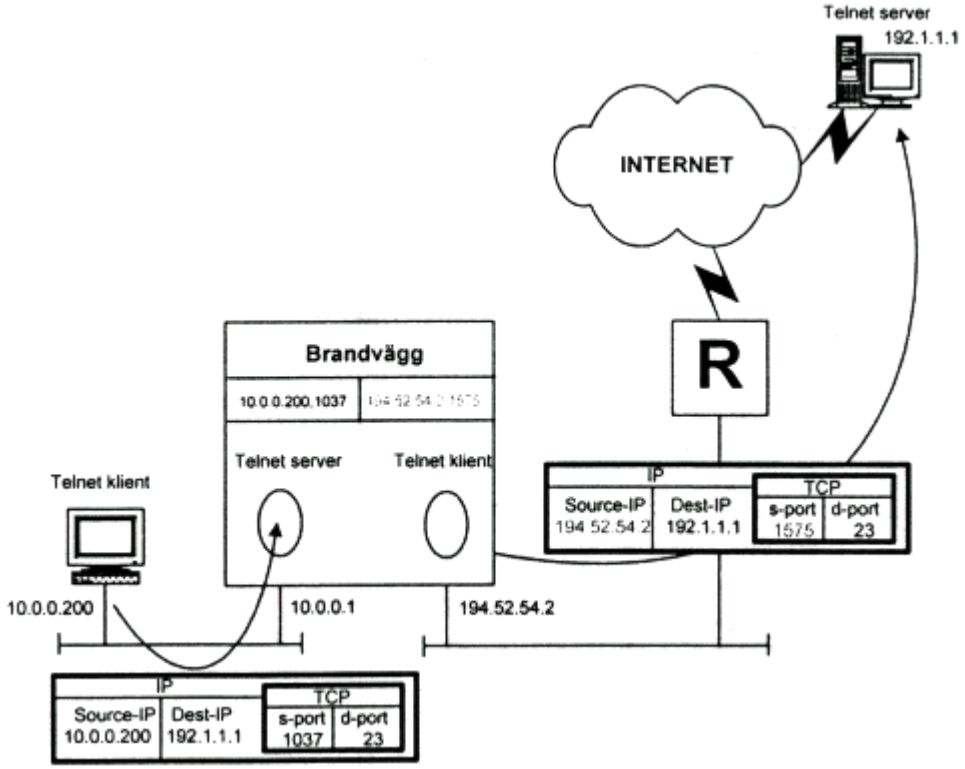


Kräver anpassning av alla klienter

Samtliga klienter som skall gå igenom brandväggen måste ha en klientprogramvara. Detta medför mycket administration.

- Klienten påbörjar en uppkoppling mot brandväggen
- Brandväggen följer regellistan som gäller för trafik och hostar.
- Brandväggen gör uppkopplingen mot begärd destination, och verifierar uppkopptingen till klientenprogrammet.
- All trafik går via brandväggen under hela sessionen.

Transparent firewall



Transparent firewall på TCP-koppelnivå

Klienterna behöver inte konfigureras. Klienterna går till brandväggen som 'default' router.

PAT (Port Adress Translation)

Brandväggen går alltid ut med samma source IP för alla översatta adresser och måste därmed byta ut även source port.

NAT (Network Address Translation)

Brandväggen får en pool av legala adresser som den knyter till de översatta adresserna. Detta är ett måste för vissa tjänster på Internet som t.ex. IRC, ICO. FTP. som bara tillåter en inloggning per IP-adress.

Statisk

Påminner om NAT men datorer på insidan får alltid samma legala adress på utsidan. Ett måste för att kunna släppa in trafik till t.ex. servrar.

Svartnat (privata nät)

Tack vare att brandväggen gör en översättning får vi möjlighet att använda svartnat för nätverk bakom brandvägg med NAT. Detta sparar IP adresser. Svartnät finns specificerade I RFC 1918.

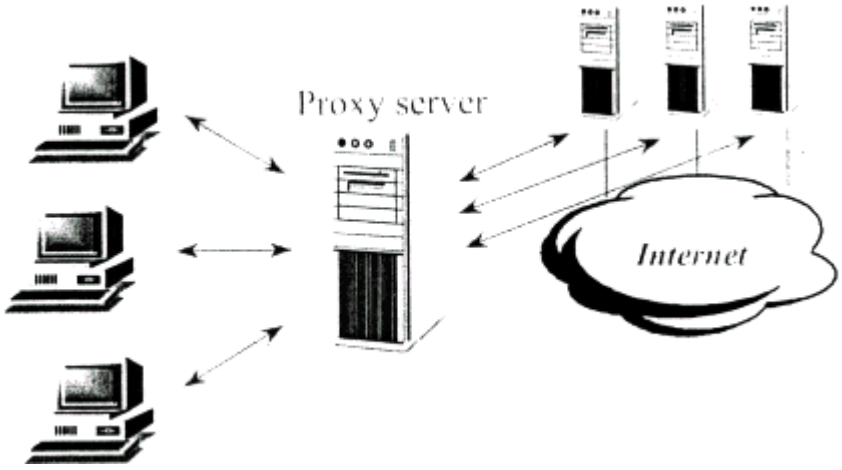
Svartnät enligt RFC 1918:

- KlassA 10.0.0.0/8
- KlassB 172.16.0.0 - 182.21.255.255/12
- KlassC 192.168.0.0 - 192.168.255.255/16

Applikationsproxy

Kräver serverstöd för varje applikation.

Kräver klientstöd



Applikationsproxy

- kan ta beslut på alla nivåer i *OSI-7* modellen
- långsam
- inkluderar cachefunktioner

Serverstöd

För varje applikation krävs stöd i servern. Detta medför att nya applikationer inte kan användas.

Klientstöd

Varje klient måste ha ett program för proxyfunktionen.

Vad är bäst?

- Paketfiltrering
- TCP-koppelnivå
- Applikationsproxy

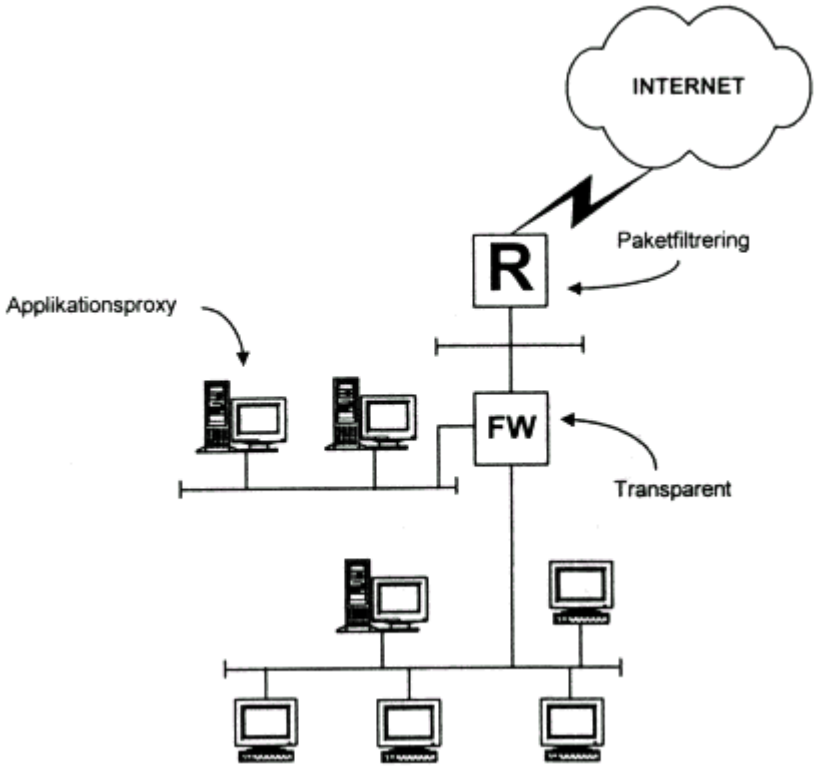
Att ta filterbeslut?

- ***Snabb!***
- ***Långsam!*** .

Beslutsmöjlighet?

- ***Stor!***
- ***Liten!***

Kombinera



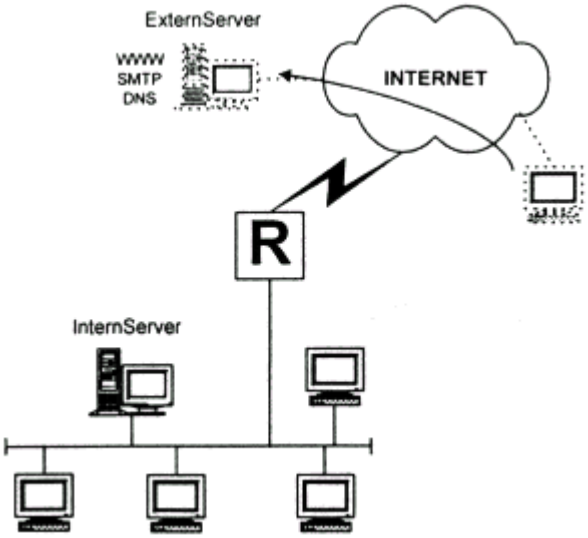
Kombinera alla typer av brandväggar:

Paketfiltrerande brandvägg som första filter mot ex winnuke. SYN-ftood och olika former av illegalt sammansatta IP paket.

Transparent brandvägg där huvuddelen av filterreglerna är applicerade.

Applikationsproxy för t.ex. WWW. Vilket gör att du kan filtrera bort JAVA, ActiveX, får cachemöjligheter.

Endast utgående trafik

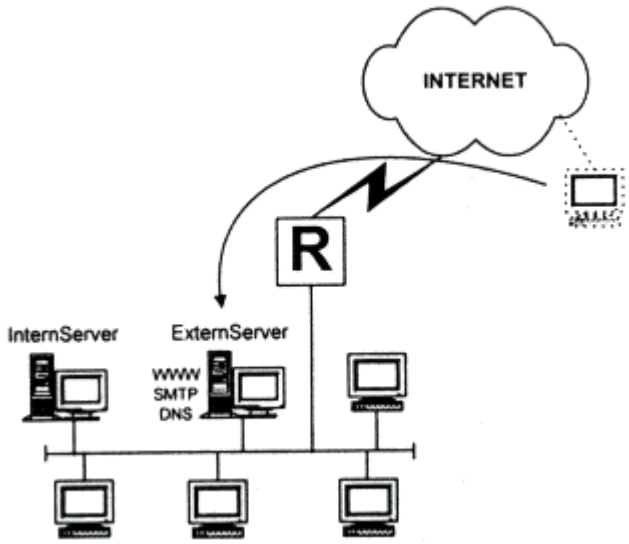


Detta är den enklaste formen av skydd. Och innebär att vi måste låta ett externt Företag sköta våra externa tjänster *såsom* WWW, SMTP och DNS.

Detta är den bästa lösning i förhållande till pris eftersom routern *redan* finns där. Det som krävs är kunskap om hur routingfiler fungerar. Duger utmärkt åt *små* och medelstora företag som ett första steg mot ett säkrare nät.

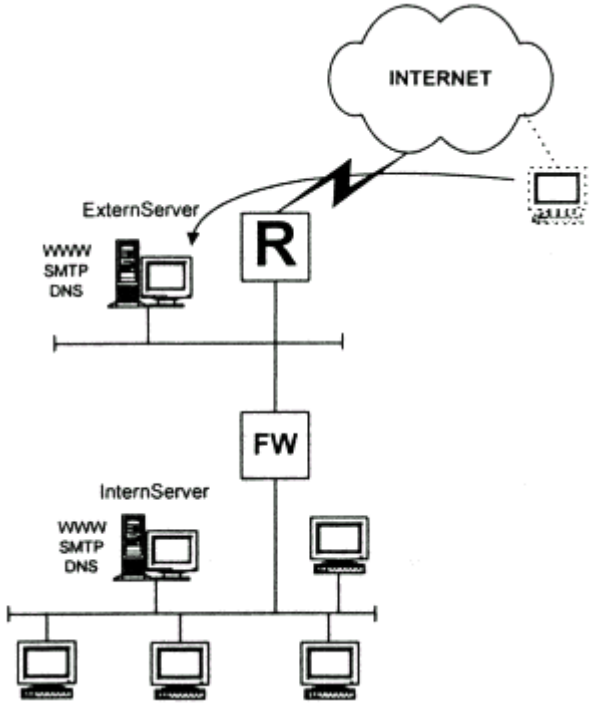
Vanligen är uppkopplingen av formen xDSL eller ISDN.

Extern server i inre nätet



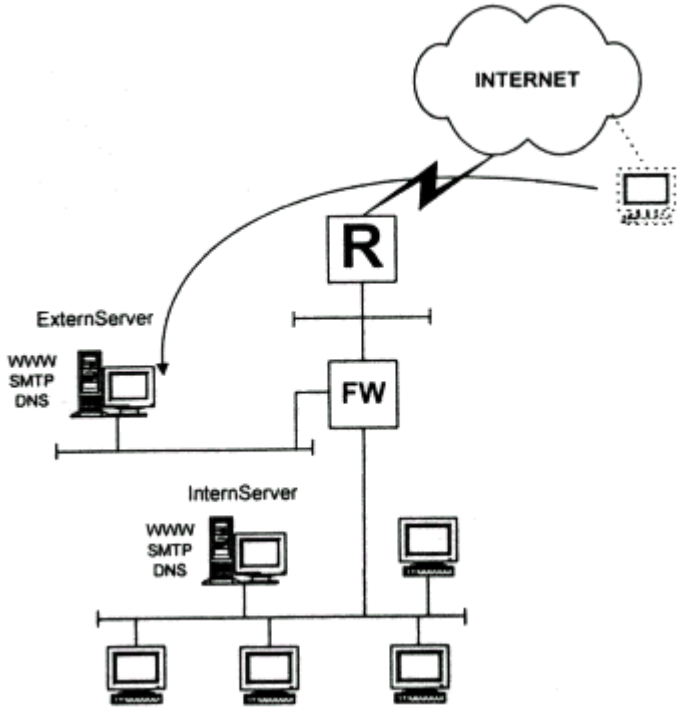
I detta fall väljer vi som företag att själva administrera de externa tjänsterna.

Extern server, yttre nät



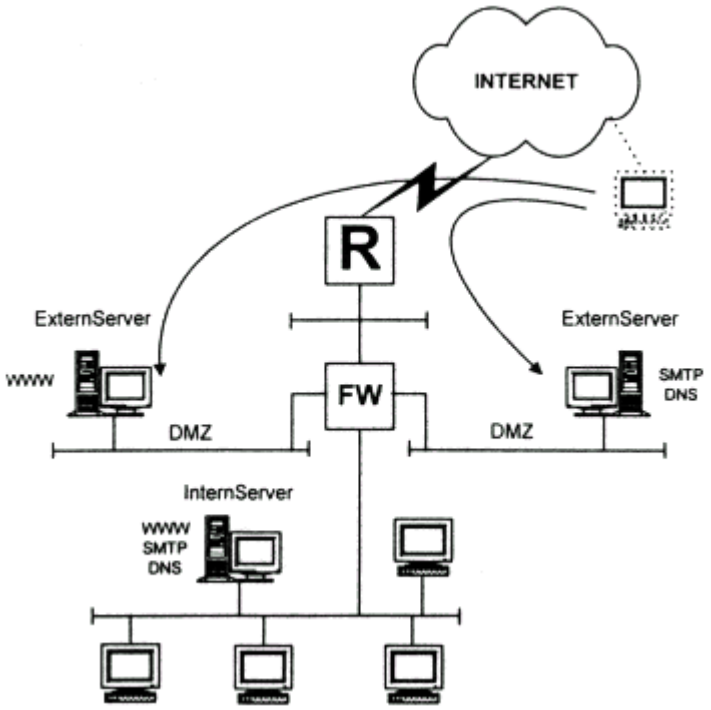
Nästa steg blir att inskaffa en brandväggsprodukt, Detta är givetvis bättre, men om externservern skulle forceras går det att analysera trafik som generaras utåt.

Brandvägg med tre interface



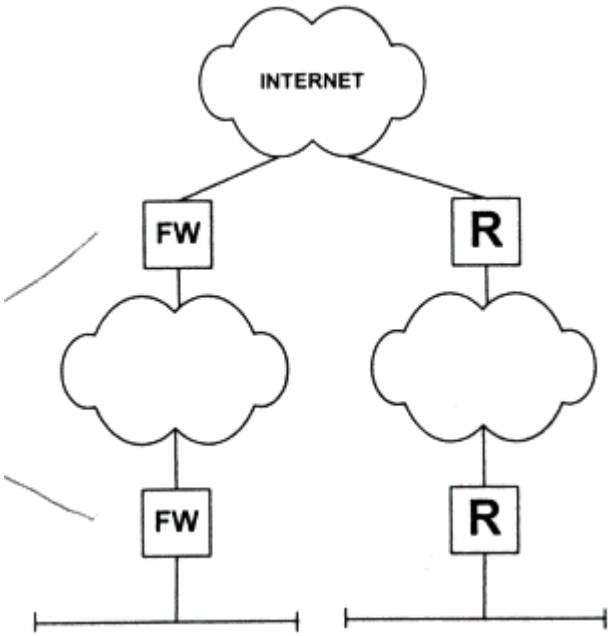
Delta *är* del vanligaste fallet och innebär *att* om externservern skulle forceras kommer det inte *att* gå att analysera trafik som genereras inifrån och ut på Internet.

Flera interface



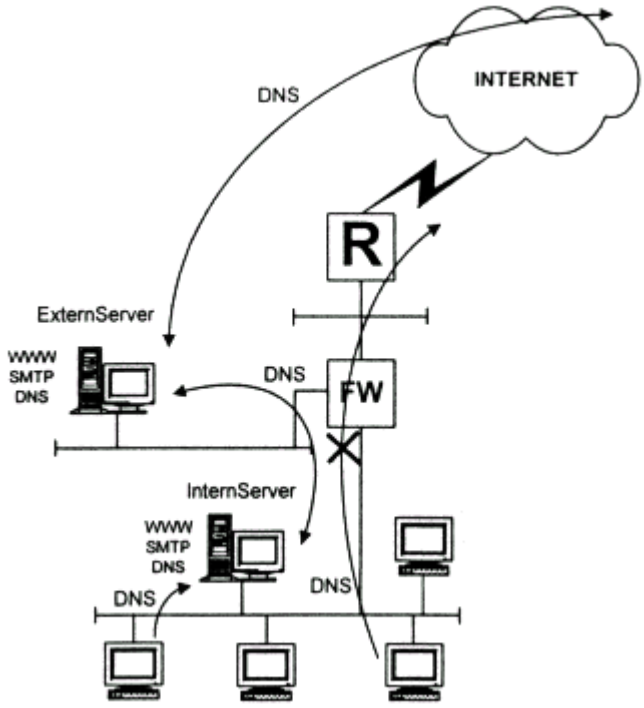
De flesta brandväggar på marknaden kan hantera mer än tre interface. Detta skulle medföra att vi kan dela upp de servarna som erbjuder tjänster till Internet. Det *är* lättare att *strukturera,* och om den ena servern skulle bli forcerad är det svårare att forcera nästa. Problemet är att brandväggen blir långsammare ju fler interface vi använder, vilket kan medför *en* större kostnad i form av dyrare hårdvara.

Dubbla FW, OS



Med dubbla brandväggar och olika operativsystem ökas säkerheten ytterligare. Man kan ha olika regler i de två brandväggarna för att tillåta olika nivåer av skydd.

Inre och yttre **servrar**



Brandväggen

I brandväggan sätter vi upp regler så att endast internservern och externservern får kommunicera med varandra. Allt annat nekas.

Klient

Eftersom klienterna inte får gå ut genom brandvaggen tvingar vi dem att gå till internserven. Detta görs genom konfigurering ex DNS -> i TCP/IP slacken.

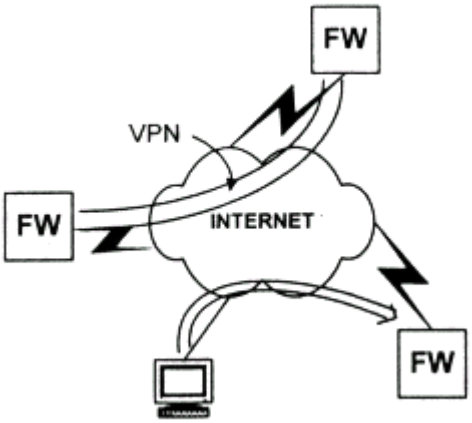
Internserver

Har som uppgift att ta mot frågor från klienterna. Om servern inte klarar av att svara på frågan skall den vidarebefordras genom brandväggen till Externservern. Ex i DNS *görs* detta med kommandot forwarders.

Externserver

Har som uppgift att dels ta emot frågor från internservern samt att svara på frågor från Internet.

VPN



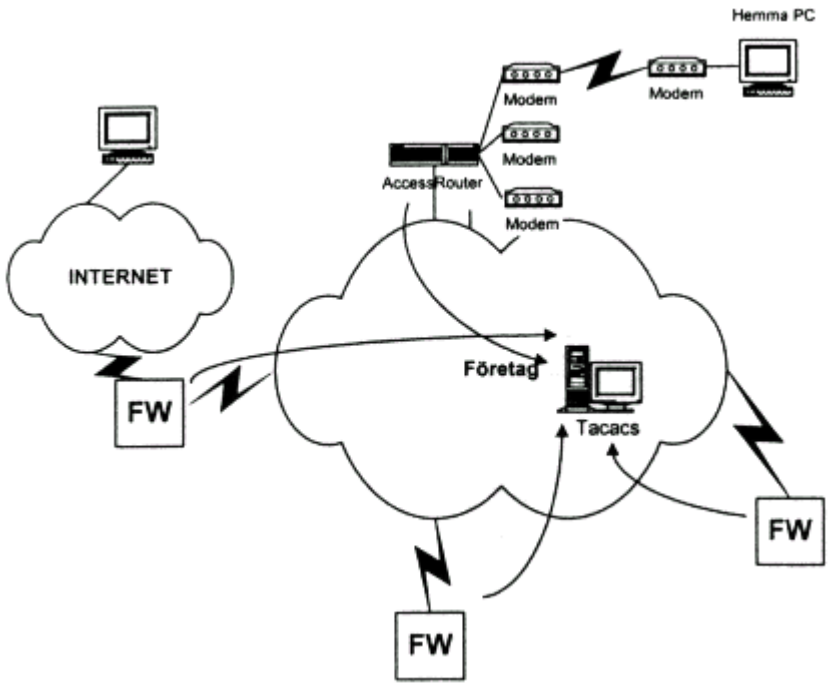
***VPN* (Virtual Private Network)**

Är något som finns implementerat i de flesta brandväggs produkter. Tekniken bygger på alt man skapar sig en krypterad tunnel mellan produktema via Internet, i stället för att hyra en dyr WAN -förbindelse. Problemet ligger i att det inte finns någon standardiserad teknik for VPN mellan skilda fabrikat, utan man tvingas *att* köpa samma produkt på alla orter. Detta leder till *att* företaget binder sig till en produkt.

Tunnling

Det senaste inom brandväggs tekniken för *att* låta anställda komma åt det intema *nätet* via Internet. Företaget behöver inte några modempooler utan kan istället teckna avtal med olika ISP'er runt om i värden. Tunnling löses med protokoll av typen Layer2Forwarding (Cisco), Point to Point Tunneling Protokoll (Microsoft) eller L2TP som är standardised. Dessa bygger på *att man* utnyttjar TCP/IP (Internet) som i sin tur nyttjar länk protokollet PPP. När det gäller kryptering löses det med standardiserade protokoll så som SSH.

Autenticering



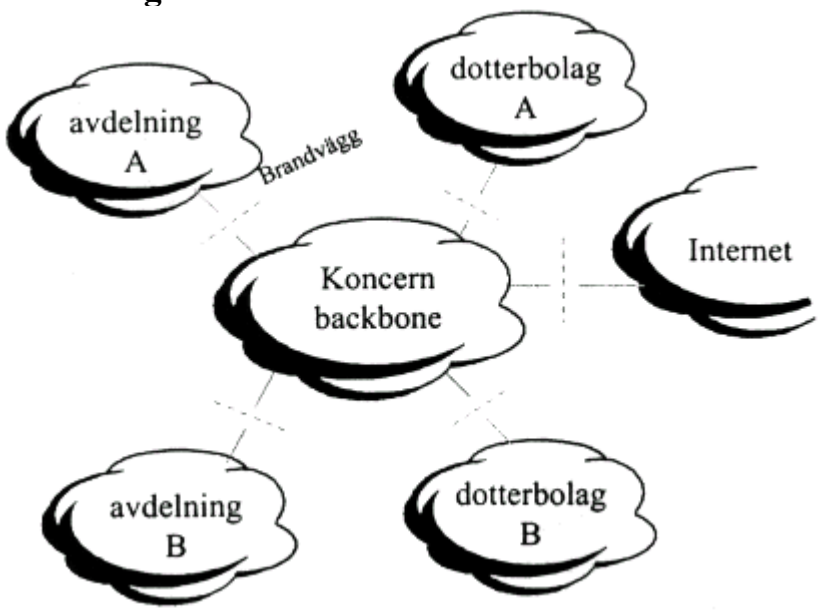
Autenticering

Används för att låta externa användare komma åt det interna nätet. Det finns två scenarier. En användare befinner sig på Internet och vill komma åt det interna nätet, eller att förataget har en modempool som användare kan ringa till. Systemansvarige lägger upp en kontodatabas för de produkter som är inblandade. Problemet infinner sig i större lösningar där det kan vara en ide att ha en central databas. Exempel på sådana lösningar är Tacacs resp. Radius. I stället för att accessroutrarna autenticerar själva skickar de vidare frågan till autenticeringserver som verifierar.

Accessrouter

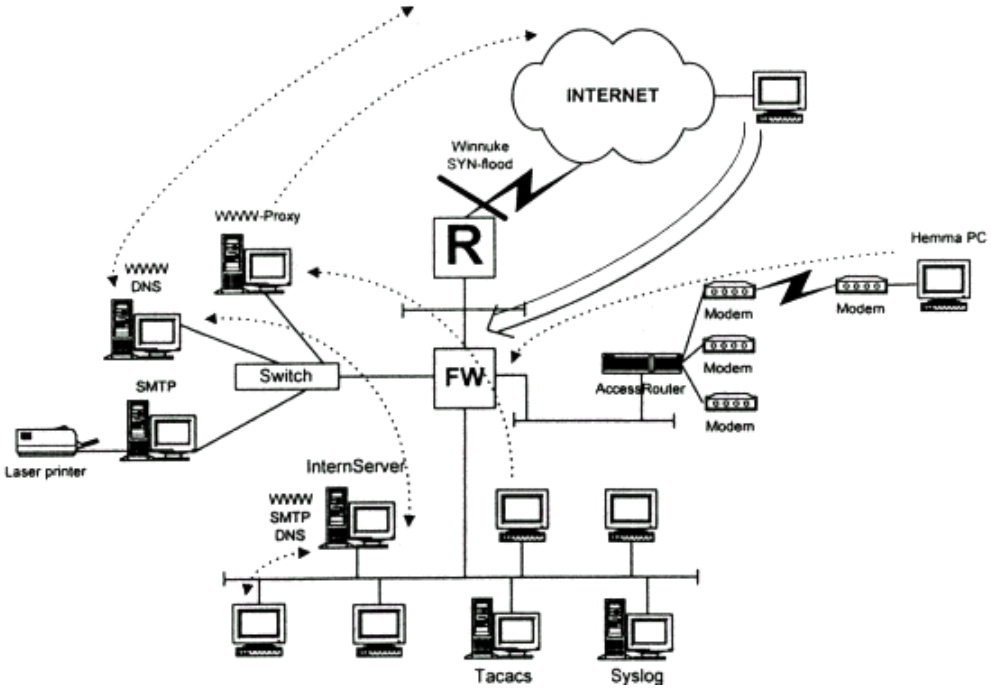
Är ett stort säkerhetsproblem i dagens företag eftersom de oftast sitter på det interna nätet, vilket ger direkt tilltgång till Företagets interna nätverk. Dessa har oftast inga filter, vilket leder till att det går att använda samtliga nätverksprotokoll. Felkonfigureringar förekommer i routrarna t.ex. att alla nätverksprotokoll är påslagna. Accessroutern bör flyttas ut till dmz.

Stora företag



När del gäller stora företag kan det internt förekomma brandväggar inom företaget. Detta kan bli väldigt komplext och måste skötas centralt. Det skulle inte fungera om var och en av avdelningarna skulls sköta sina egna brandväggar.

Helhetslösning



Internet router
Ägs oftast av Internetleverantören, och det är därför viktigt att man har kunskap och kan hantera en dialog med dem. Här bör det installeras filter mot Netbiosportarna 137,138,139, samt skydda mot SYN flood attacker.

Access router
Är till för de anställda för att kunna jobba på distans. Problemet med dagens företag är att denna ofta står på det interna nätet utan filter och kanske IPX och NetBIOS påslaget. Genom att flytta ut den till en anslutning på brandväggen kan vi enkelt filtrera, autenticera i brandväggen eller mot en radius-server. Det är även lättare att följa upp med loggar.

Loggning
Skall på ett säkert sätt föras in i företaget helst genom kryptering och filter som öppnar endast under de tider cron-jobbet startar. Cron-jobb är schemalaggda jobb i en UNIX-maskin.

Skrivare
Skrivarens uppgift är att säkerställa en loggning. Det finns inga möjligheter att radera loggspår om inte man har fysisk tillgång till skrivaren. Denna lpggning skall användas vid kritiska maskiner och förekommer inom bankvärlden.

Switch
Tanken med switcben är att om någon server blir attackerad på dmz skall det försvåra sniffning av nätverket. Altemativet hade varit att ha flera gränssnitt på brandväggen men detta skulle medföra att vi skulle få en högre kostnad på brandväggen.

Externa och Interna-servrar
Skall i så stor utsträckning som möjligt implementeras. För t ex. DNS SMTP...

Brandvaggen
Skall filtrera så mycket som möjligt utan att hindra tillgängligheten

Sammanfattning

Brandväggens uppgift är *att* minska riskområdet för hostar och tjänster.

"Falsk trygghet (hårt skal med mjukt innehåll)". .
Om brandväggen förstörs då ökar riskområdet.

Kommersiella brandväggar

- Snabb kommersialisering sedan 1995 ca 50 olika produkter
- Firewall-1
- PIX Firewall
- **Gauntlet**
- **Fuego**
- Altavista Firewall
- Watchguard
- Radguard

Firewall-1 (Mjukvara, Son, HP, NT) Checkpoint
http://www.checkpoint.com
Salcom Communication AB http://www.salcom.se/
PIX Firewall (Hardvara. P233, BSD!) Cisco
http://www.cisco.eom/warp/public/751/p:x/
Telia Megacom AB http://www.telia.se/megacom/
Gauntlet (Mjukvara, Sun Hp BSDI) Trusted information Systems
http://www.tis.com/
Medcom http://www.medcom.se
Fuego Firewall (Hardvara, nee, Linux)
Signum Support AB http://www.signum.se
Altavista friewall 98 (Mjukvara, NT, Digital UNIX)
Digital http://www.aitavista.software.digital.com
Digitaipartner http://www.digitalpartner.se/
Watchguard Firebox II (Hardvara, Linux)
Watch Guard http://www.watchguard.com
Data Construction http://www.dc.eiknes.se/
Radguard (Hardvara) Radguard http://nww.radguard.com
Arecia http://www.arecta.se

Att utvärdera brandväggar

- Systemmiljö och leverantör
- Kostnader
- Antal interface
- Flera brandväggar
- Admin och Monitoreringsmöjlighet och andra funktioner
- Servertjänst

System miljö och leverantör

- Unix. NT
- Telia. Digital. IBM, ...

Kostnader

- HW
- Programvara
- Administration
- Konsulthjälp

Admin och Monitoreringsmöjlighet Användbarhet

- Normal trafik
- Vid incident

Användbarhet

- Hantering och olika tjänster samt protokoll

Servertjänst

- Krypleradeftrbindelser