Firewalls

Firewalls

drs. ing. R. Pluis MBA MBI CISSP (redactie)

Uitgeverij LEMMA BV – Utrecht – 2005

Aan de totstandkoming van deze uitgave is de uiterste zorg besteed. Voor informatie die nochtans onvolledig of onjuist is opgenomen, aanvaarden auteur(s), redactie en uitgever geen aansprakelijkheid. Voor eventuele verbeteringen van de opgenomen gegevens houden zij zich gaarne aanbevolen.

Ondanks de nodige nasporingen bleek het niet mogelijk van alle opgenomen illustraties de bezitter van het copyright te achterhalen. Eventuele rechthebbenden die niet voor deze uitgave zijn benaderd, wordt verzocht zich met de uitgever in verbinding te stellen.

ISBN 90 5931 3526
NUR 980

http://www.lemma.nl
infodesk@lemma.nl

Omslagontwerp en typografie: Twin Design BV, Culemborg

Voorwoord

Het Platform Informatiebeveiliging (PI) heeft als doel 'het bevorderen van de beveiliging van alle belangen betreffende gegevensverwerking, -opslag en -transport, alles in de ruimste zin van het woord'. Binnen deze doelstelling wordt het ontwikkelen van aanvaardbare richtlijnen voor de praktische inrichting van informatiebeveiliging als essentieel onderwerp gezien. Door het gezamenlijk opstellen van dergelijke richtlijnen kan gebruikgemaakt worden van praktijkervaringen, zodat een doeltreffende richtlijn ontstaat die ook uitvoerbaar is.

De PI-richtlijnen worden in werkgroepverband ontwikkeld onder auspiciën van een bestuurslid in de rol van projectleider. Deze ziet er onder meer op toe dat de PI-kwaliteitsrichtlijnen door de werkgroep worden gehandhaafd. De deelnemers van de werkgroepen zijn primair afkomstig uit de organisaties die aangesloten zijn bij PI, maar niet uitsluitend. Alle deelnemers zijn beveiligingsfunctionarissen en IT-auditoren van uiteenlopende bedrijven en instellingen, die zich kenmerken door de hoge eisen die zij in hun advies- en controlewerkzaamheden aan organisaties moeten stellen in verband met de sterke automatiseringsgraad en de belangen die met de geautomatiseerde informatievoorziening zijn gemoeid. Door hun achtergrond vormen de deelnemers een representatieve afspiegeling van de aanwezige IT-beveiligingsexpertise in Nederland en bieden zij een draagvlak om gezag te verlenen aan de ontwikkelde richtlijnen, hetgeen bevorderlijk is voor de acceptatie door het algemeen en het IT-management.

De PI-beveiligingsrichtlijnen zijn primair bedoeld voor functionarissen die zijn belast met het implementeren van IT-systemen, zoals systeembeheerders, technische ontwerpers en bouwers. Daarnaast zijn de richtlijnen van betekenis voor de volgende doelgroepen:

– IT-beveiligingsfunctionarissen (*security officers* en *administrators*): de IT-beveiligingsfunctie binnen een organisatie is verantwoordelijk voor het (doen) treffen van beveiligingsmaatregelen. De richtlijnen bieden hierbij ondersteuning.
– IT-management: het IT-management is (eind)verantwoordelijk voor de informatiebeveiliging binnen zijn competentiegebeid en geeft hieraan invulling door het (doen) analyseren van risico's en het bepalen van (globale) beveiligingsdoelstellingen. De beargumenteerde keuzen in de richtlijnen kunnen als handvatten worden gebruikt.
– IT-auditoren: de richtlijnen kunnen worden gehanteerd als toetsingsnorm bij IT-audits.

Aldus bieden de richtlijnen enerzijds een handreiking aan beveiligingsfunctionarissen en het IT-management om een toereikende en evenwichtige beveiliging van de informatievoorziening te implementeren en bieden zij anderzijds een basis aan IT-auditoren voor de normstelling bij de beoordeling van de beveiliging van een IT-systeem.

Norea, de beroepsorganisatie van IT-auditoren, beoogt met het in 2002 gepubliceerde *Studierapport 3* (getiteld: *Raamwerk voor ontwikkeling van normenstelsels en standaarden*) een extra impuls te geven aan de ontwikkeling van normen en standaarden die bij IT-audits worden gebruikt. Het Platform Informatiebeveiliging en Norea hebben gezamenlijk vastgesteld dat de PI-studies en PI-standaarden, hoewel vaak niet voldaan aan de formatvereisten van *Studierapport 3*, in deze context zeker ook voor IT-auditoren waardevolle handreikingen kunnen bevatten. In concreto is door Norea geconstateerd dat deze PI-studie *Firewalls* als handreiking kan dienen bij het uitvoeren van IT-audits. Wij bevelen de publicatie dan ook van harte aan aan onze leden.

De inhoud van de PI-studie *Firewalls* is totstandgekomen in nauwe samenwerking met de PI-projectwerkgroep, tijdens een aantal zogenaamde *eXtreme Writing*-sessies die bij Capgemini Nederland gehouden zijn. Tijdens deze sessies werd in een extreem korte tijd (meestal drie dagen) een groot aantal pagina's geschreven of verder uitgewerkt. In uiterste concentratie werd onder aansturing van *facilitators* veel vooruitgang geboekt. In tegenstelling tot het 'normale' eXtreme Writing-proces was er tussen de sessies ruimte om met de leden van de PI-projectwerkgroep te overleggen. Dit heeft ertoe geleid dat de ruwe inhoud van boek, na de voorbereidende werkzaamheden die door de PI-projectwerkgroep en het aanspreekpunt van Capgemini zijn uitgevoerd, in relatief korte tijd geschreven is. Het boek is voltooid na een aantal workshops met zowel de PI-projectwerkgroep als de PI-leden.

Inhoud

1 Inleiding

De toenemende integratie van automatisering met de bedrijfsprocessen en de eveneens toenemende complexiteit van automatiseringsoplossingen noodzaken tot voortdurende aandacht voor zowel het vereiste niveau van informatiebeveiliging als de technische realisering hiervan. Ook gezien de ontwikkelingen op het gebied van wet- en regelgeving met betrekking tot informatiebeveiliging is deze aandacht noodzakelijk.

Objectivering van het vereiste niveau van informatiebeveiliging en van de effectiviteit van gekozen technische oplossingen is voor veel organisaties een probleem, omdat slechts in beperkte mate standaarden voorhanden zijn. Beschikbare standaarden kennen ofwel een te beperkt werkingsgebied, of richten zich te veel op de organisatorische kant van de informatiebeveiliging. Door het gebrek aan deugdelijke standaarden zijn organisaties gedwongen zelf oplossingen te ontwikkelen en hierin veel energie te steken. De gevolgen zijn suboptimale oplossingen, verspilling – doordat vele malen opnieuw het wiel moet worden uitgevonden – en moeizame acceptatie, door de afwezigheid van geobjectiveerde criteria.

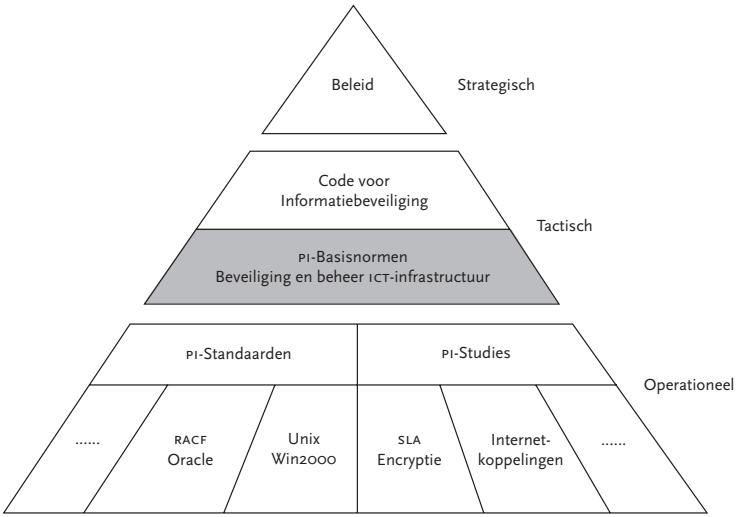
Tegen deze achtergrond is het initiatief ontstaan om in werkgroepverband concrete, geobjectiveerde richtlijnen te ontwikkelen voor de inrichting respectievelijk de beoordeling van technische beveiligingsmaatregelen. Deze aanpak heeft de volgende voordelen:

- Door uitwisseling van kennis, ervaring en inzicht ontstaat een belangrijk synergie-effect tussen de deelnemers; de deelnemers kunnen elkaar ondersteunen bij de keuze en implementatie van beveiligingsmaatregelen.
- Met behulp van de ingebrachte kennis en inzichten kan worden gekomen tot de vaststelling van technische beveiligingsrichtlijnen die op een breed draagvlak kunnen rekenen.

– Toepassing van de opgestelde beveiligingsrichtlijnen leidt bij de betrokken organisaties tot een verhoging van de effectiviteit van de beveiliging.

De technische beveiligingsmaatregelen die in de richtlijnen worden beschreven, vormen een onderdeel van de bredere context van het gehele samenstel van beveiligingsmaatregelen om de kwaliteit van de geautomatiseerde informatievoorziening te waarborgen.

Beveiligingsmaatregelen binnen deze bredere context zijn bijvoorbeeld beschreven in de publicatie *Code voor Informatiebeveiliging*[1]*, een Standaard voor Beleid en Implementatie*, een internationale *best practice* (ISO/IEC 17799:2000). Deze *Code*, die vooral in het bedrijfsleven wordt gebruikt, richt zich in het bijzonder op het tactische niveau binnen organisaties en bestrijkt het gehele terrein van informatiebeveiliging. Door het abstractieniveau geeft de *Code* echter weinig concrete handvatten voor het implementeren van beveiligingsmaatregelen bij IT-systemen. Hetzelfde geldt nog sterker voor het besluit *Voorschrift Informatiebeveiliging Rijksdienst* (*VIR*)[2], dat op de rijksoverheid van toepassing is.



Figuur 1.1 Informatiebeveiligingspiramide

De PI-richtlijnen kunnen dan ook worden beschouwd als een verdere praktische uitwerking van de *Code* en de baselinebeveiliging van het besluit *VIR*, en zijn vooral gericht op het operationele niveau binnen organisaties. Daarnaast kan nog een strategisch niveau worden onderkend, dat betrekking heeft op de eindverantwoordelijkheid voor informatiebeveiliging van het topmanagement. De samenhang tussen deze drie niveaus is schematisch weergegeven in figuur 1.1.

Aangezien voor het tactische niveau van informatiebeveiliging en voor de beleidsmatige en organisatorische maatregelen die op het strategische en tactische niveau moeten worden getroffen, al veel literatuur voorhanden is, wordt hierop in de PI-richtlijnen niet nader ingegaan. Het uitgangspunt van de PI-richtlijnen is dat op dit gebied voldaan is aan de *Code voor Informatiebeveiliging* en vergelijkbare standaarden, alsmede aan de *Basisnormen Beveiliging en Beheer IT-infrastructuur*, die hiervan op het relevante deelgebied een nadere invulling geven. Dit houdt in dat er een beveiligingsbeleid is, dat er functiescheiding is tussen ontwikkeling en productie, et cetera.

Bij de implementatie van een product of architectuur moet een evenwicht worden gevonden tussen risico's enerzijds en een daarmee samenhangend beveiligingsniveau, invoerings- en beheerkosten en gevolgen voor de prestaties van het systeem anderzijds. De richtlijnen bieden hierbij een praktische leidraad, doordat beargumenteerd wordt aangegeven waarom bepaalde keuzen zijn gemaakt. Door deze aanpak kunnen organisaties de vertaalslag maken naar hun eigen specifieke omstandigheden.

1.1 PI-beveiligingsrichtlijnen

De beveiligingsrichtlijnen die in PI-verband zijn en worden ontwikkeld, betreffen de technische maatregelen en voorzieningen die men moet treffen ter waarborging van de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens die met een IT-systeem worden opgeslagen, verwerkt en/of getransporteerd.

De richtlijnen geven dus aan hoe de (beveiligings)functies van een IT-systeem, die relevant zijn voor de genoemde kwaliteitsaspecten, moeten worden ingesteld. Zij bevatten tevens aanwijzingen voor de organisatorische inbedding hiervan, maar primair gaat het om de techniek.

Met de richtlijnen wordt vooral beoogd te bevorderen dat de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens in voldoende mate zijn gewaarborgd. Dat wil niet zeggen dat andere kwaliteitsaspecten, zoals efficiëntie (bedieningsgemak, performance, kostenbeheersing), uit het oog worden verloren. Juist door de inbreng vanuit de praktijk wordt gestreefd naar een optimaal evenwicht tussen beveiligingsniveau en praktische realiseerbaarheid. De richtlijnen vormen de neerslag van de gezamenlijke kennis, inzichten en praktische ervaringen van de werkgroepen en PI-leden.

De richtlijnen kunnen betrekking hebben op elke component van de IT-infrastructuur in de breedste zin van het woord (aangeduid als IT-systeem). De IT-infrastructuur betreft het geheel van apparatuur, besturings- en hulpprogrammatuur, faciliteiten voor data-, spraak- en videocommunicatie, alsmede de fysieke beveiligingsfaciliteiten van de geautomatiseerde informatievoorziening. Ook generieke toepassingen en diensten (zoals e-mail en filetransfer) vallen onder het begrip 'IT-systeem'.

De beveiligingsrichtlijnen van PI vallen uiteen in twee categorieën:
- PI-standaarden: PI-standaarden zijn technische implementatiehandleidingen voor concrete objecten (IT-componenten), bijvoorbeeld een besturingssysteem van een bepaalde leverancier en een bepaalde versie.
- PI-studies: PI-studies zijn technische beveiligingshandleidingen voor objecttypen, bijvoorbeeld een bepaalde categorie besturingssystemen, generieke IT-architecturen, bijvoorbeeld een firewall, internetverbinding of inbelfaciliteit en generieke diensten, bijvoorbeeld directoryservices.

Bij nieuwe versies van IT-componenten en bij nieuwe technologische of maatschappelijke ontwikkelingen bestaat er behoefte aan vroegtijdige risico-inschatting en standpuntbepaling met betrekking tot de invulling

van beheer- en beveiligingsaspecten. In die gevallen zijn de richtlijnen meer het resultaat van een researchinspanning dan dat zij – zoals bij bestaande IT-componenten en architecturen – zijn gebaseerd op langdurige eigen praktische ervaring.

Het te bereiken beveiligingsniveau dient te zijn afgestemd op de waarde van het te beveiligen belang. Aangezien dit voor elke organisatie verschillend zal zijn, zijn de PI-richtlijnen primair gebaseerd op de beveiligingsmogelijkheden van het IT-systeem, dat wil zeggen op het optimaal benutten van de beveiligingsfaciliteiten die het systeem biedt. Dit wordt het beginsel van goed huisvaderschap genoemd. Bij het opstellen van de richtlijnen wordt echter tevens nagegaan aan welk niveau het systeem redelijkerwijs zou moeten voldoen, gegeven de *Code voor Informatiebeveiliging* en andere gezaghebbende literatuur, de *state of the art* van de beveiligingstechniek, de gemeenschappelijke *common sense* van de werkgroepleden, enzovoort.

1.2 Uitgangspunten voor deze PI-studie

Bij het lezen van deze studie dienen de volgende uitgangspunten in acht te worden genomen:

> ***Uitgangspunt 1:*** *In deze firewall-studie worden firewall-functionaliteiten behandeld als een middel om netwerkverkeer tussen domeinen met verschillend beveiligingsniveau te reguleren.*

In de formulering van dit uitgangspunt ligt een zeer breed scala aan mogelijke verschijningsvormen van firewalls opgesloten. Verreweg de bekendste vorm is die van een firewall die wordt gebruikt om het bedrijfsnetwerk te koppelen aan het internet. Echter, de hier behandelde theorie en benadering zijn evengoed van toepassing op het reguleren van netwerkkoppelingen tussen alle mogelijke domeinen. Dit betekent dat ook verschijningsvormen zoals de *personal firewall* (een scheiding tussen de pc en een netwerk) en de intranet-firewall (een scheiding tussen twee interne netwerken) worden gedekt door deze studie.

> ***Uitgangspunt 2:*** *Deze firewall-studie moet worden beschouwd als een nadere uitwerking van de* PI*-studie Basisnormen Beveiliging en Beheer* IT*-infrastructuur.*

Dit uitgangspunt is bepalend voor de reikwijdte van de uitwerking. In deze firewall-studie worden alleen die onderwerpen nader uitgewerkt, die voor dit onderwerp om een verdere verdieping vragen. De basisnormen uit de PI-studie *Basisnormen Beveiliging en Beheer* IT*-infrastructuur*, die in het bijzonder van toepassing zijn op firewalls, hebben we dan ook gerecapituleerd in het hoofdstuk waarin de basismaatregelen zijn uitgewerkt.

> ***Uitgangspunt 3:*** *In de* PI*-studie Internet worden risico's en maatregelen behandeld van de toepassingsmogelijkheden van internet, die bepalend zijn voor de inrichting van de firewall, die de koppeling van het internet met het interne netwerk reguleert.*

De inrichting van een firewall wordt mede bepaald door de risico's en de belangen die samenhangen met de toepassingen, die over de te reguleren netwerkkoppeling lopen. Het valt buiten het kader van deze PI-studie om daar op in te gaan. Voor de koppeling van het internet met het interne netwerk heeft PI een aparte studie uitgebracht. In versie 2 van deze PI-studie wordt zeer kort op firewalls ingegaan. Versie 3 van deze studie zal hiervoor naar de PI-studie *Firewalls* verwijzen.

> ***Uitgangspunt 4:*** *In deze firewall-studie wordt het* ISO-OSI*-abstractielagenmodel gebruikt als theoretisch referentiekader en het* TCP/IP*-model als realisatie-referentiekader.*

In de tekst van deze studie wordt afwisselend gesproken over het ISO-OSI-model, dat goed geschikt is om de theorie en de verschillende abstractielagen te beschrijven, en over het TCP/IP-model, indien er voorbeelden worden gegeven van bepaalde realisaties. Deze modellen worden bewust naast elkaar gebruikt. Het zal uit de tekst blijken welk model van toepassing is.

Uitgangspunt 5: *In deze firewall-studie wordt alleen het netwerkprotocol IP versie 4 behandeld.*

Deze studie richt zich op versie 4 van het Internet Protocol. Hoewel IP versie 6 met enige mate toegepast begint te worden op het internet en binnen enkele bedrijven, is IPv4 de huidige standaard en is er besloten om deze studie alleen op IPv4 te richten.

1.3 Leeswijzer en samenvatting

Omdat deze PI-studie vooral gericht is op IT-beveiligingsfunctionarissen en IT-auditoren is ervoor gekozen eerst de theoretische uitgangspunten (het ISO-OSI-model) in combinatie met het TCP/IP-model toe te lichten in hoofdstuk 2. Dit verschaft het kader voor een algemene bespreking van filtertechnieken in hoofdstuk 3.

Kennis van deze twee hoofdstukken is noodzakelijk voor het begrip van hoofdstuk 4, dat de functionaliteiten van een firewall beschrijft, los van de technische implementatie. Deze functionaliteiten zijn de bouwstenen voor het ontwerp van een firewall, waarvoor de ontwerpcriteria in hoofdstuk 5 worden uitgewerkt. Een logisch vervolg op het ontwerp is de implementatie, waarbij tal van nadere keuzen zijn te maken, die in hoofdstuk 6 worden besproken. Het beheer van firewalls in hoofdstuk 7 is de laatste schakel in het geheel.

In hoofdstuk 8 wordt deze studie – voor zover mogelijk – samengevat in toetsingscriteria, die als basismaatregelen worden gepresenteerd. Voorafgaand hieraan wordt in datzelfde hoofdstuk de relatie gelegd met de PI-studie *Basisnormen Beveiliging en Beheer IT-infrastructuur*.

Noten

1 De *Code voor Informatiebeveiliging* is een uitgave van het Nederlands Normalisatie-instituut, mogelijk gemaakt door het Ministerie van Economische Zaken in samenwerking met een groep toonaangevende bedrijven en organisaties in Nederland.

2 Het besluit *Voorschrift Informatiebeveiliging Rijksdienst 1994* is uitgegeven door het Ministerie van Binnenlandse Zaken in samenwerking met een begeleidingsgroep waarin alle ministeries en enkele toonaangevende organisaties waren vertegenwoordigd.

2 Het ISO-OSI-model en het TCP/IP-protocol in hoofdlijnen

In dit hoofdstuk worden twee fundamentele netwerkbegrippen geïntroduceerd, die nodig zijn om firewalls te begrijpen. Eerst wordt het ISO-OSI-model gepresenteerd en daarna het TCP/IP-protocol.

Het ISO-OSI-model wordt gebruikt om verschillende beveiligingstechnieken met elkaar te vergelijken en hun voordelen en nadelen te bespreken. Vrijwel alle modellen en technieken van firewalls passen op de lagen 3, 4 en 7 van ISO-OSI (netwerk-abstractielaag, transport-abstractielaag en applicatie-abstractielaag). Het OSI-model is bij de discussie bruikbaarder dan het TCP/IP-model. In de praktijk echter wordt het TCP/IP-protocol veelvuldig toegepast, in tegenstelling tot de OSI-protocollen.

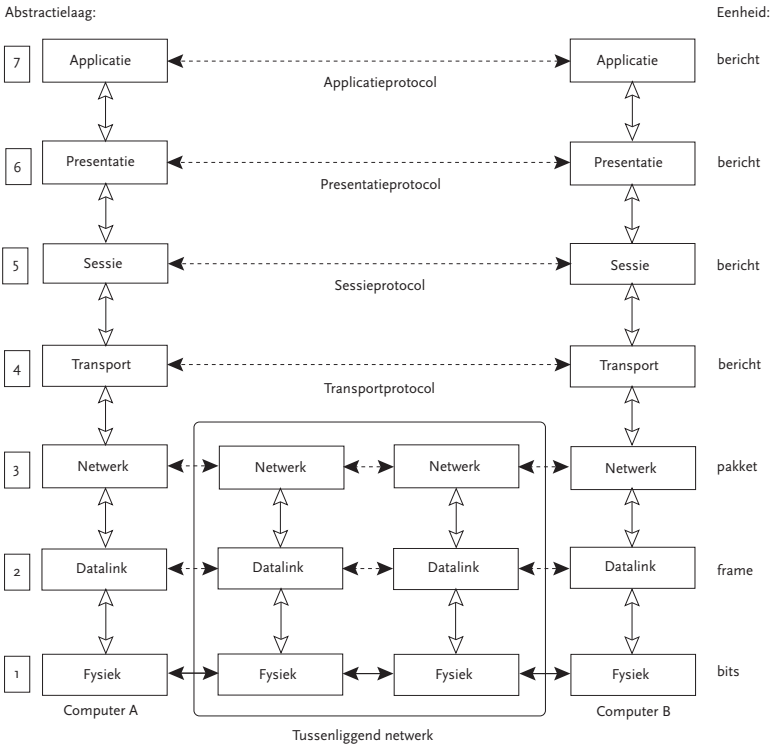
Er wordt in dit hoofdstuk alleen ingegaan op de aspecten van het ISO-OSI-model en het TCP/IP-protocol die een directe relatie hebben met firewalls en met de filtering van dataverkeer. Beveiligingstechnieken voor andere onderdelen van netwerkinfrastructuren worden niet behandeld.

2.1 Het ISO-OSI-model

Bij de ontwikkeling van het ISO-OSI-model zijn de volgende uitgangspunten gebruikt om tot zeven abstractielagen te komen:

- Elke abstractielaag moet een goed gedefinieerde en een goed afgebakende functie uitvoeren.
- De functie van een abstractielaag moet aansluiten bij gestandaardiseerde en internationaal erkende netwerkprotocollen.
- De grens van een abstractielaag moet zo gekozen worden dat met een minimum aan informatie tussen abstractielagen gecommuniceerd kan worden.

– Het aantal abstractielagen moet groot genoeg zijn om verschillende functies van elkaar te onderscheiden, maar niet zo groot dat het model onwerkbaar wordt.



Figuur 2.1 Het ISO-OSI-model

Figuur 2.1 illustreert hoe het ISO-OSI-model uit zeven abstractielagen is opgebouwd. De gebruikte symbolen kunnen als volgt worden geïnterpreteerd:

– Een *gestippelde pijl* geeft de logische communicatie tussen twee functies weer. Zo kan de cryptografische applicatie PGP bijvoorbeeld worden beschouwd als een functie die op de presentatielaag werkzaam is en gegevens doorgeeft aan de PGP-applicatie bij de ontvanger. De versturende PGP-applicatie op computer A communiceert dus

logisch gezien met de ontvangende PGP-applicatie op computer B. De daadwerkelijke informatie wordt op computer A van laag 6 naar laag 5 doorgegeven met aanvullende informatie, zodat laag 5 weet wat ermee moet gebeuren. Er vindt geen rechtstreekse communicatie plaats tussen dezelfde abstractielagen op verschillende systemen (met uitzondering van laag 1, de fysieke laag).

– Een *doorgetrokken witte pijl* geeft de vertaalslagen weer tussen abstractieniveaus op één en hetzelfde systeem. De te verzenden gegevens worden vertaald en doorgegeven tussen buffers in het geheugen van het systeem. Er is op dat moment geen extern netwerkverkeer. De abstractielaag ontvangt gegevens van de bovenliggende abstractielaag en voert de eigen functie uit op de gegevens (als dat nodig is, zo niet, dan worden de gegevens ongewijzigd doorgegeven). Daarna geeft de abstractielaag het resultaat door aan de onderliggende abstractielaag. Hierbij bestaan (uiteraard) twee uitzonderingen, namelijk abstractielaag 7 die zijn 'input' rechtstreeks van de gebruiker of van een programma ontvangt, en abstractielaag 1 die direct communiceert met abstractielaag 1 op een ander systeem.
– Een *doorgetrokken zwarte pijl* staat voor de uiteindelijke, fysieke gegevensstroom (elektrisch signaal, lichtpuls, draaggolf) die het systeem verlaat en via een netwerkverbinding wordt doorgegeven aan een ander systeem.

Zodra er informatie van computer A naar computer B gestuurd moet worden, wordt de informatie vanaf laag 7 tot aan laag 1 op computer A bewerkt en doorgegeven (zie hiervoor de volgende paragrafen). Daarna wordt de informatie fysiek verzonden naar computer B (vaak via meerdere tussenliggende computers, switches of routers). Bij ontvangst op computer B wordt de informatie vanaf laag 1 tot aan laag 7 opnieuw doorgegeven en verwerkt en wordt de informatie van computer A in ontvangst genomen.

Niet alle lagen van het ISO-model hoeven altijd doorlopen te worden. Eenvoudige applicaties en protocollen gebruiken slechts een beperkte subset van abstractielagen. Een voorbeeld hiervan is de functie 'ping' die gebruikt wordt om de verbinding tussen systemen te testen en die verder geen informatie transporteert. Deze eenvoudige functie maakt alleen gebruik van de lagen 3, 2 en 1.

In de volgende subparagrafen worden de afzonderlijke abstractielagen nader uitgewerkt en wordt ook het verband met TCP/IP aangegeven.

2.1.1 De fysieke laag

De fysieke laag houdt zich bezig met het versturen van afzonderlijke *bits* (0 of 1) tussen systemen. Deze abstractielaag heeft geen kennis van de betekenis of de structuur van de informatie die verzonden wordt. Hij ziet alleen de 'losse' bit en zorgt ervoor dat deze bit goed verstuurd wordt, waarna de volgende bit verstuurd kan worden. De fysieke laag houdt zich bezig met uiterst praktische details zoals connectoren, kabels, pulsen, voltages, frequenties en de te gebruiken timing (zoals bij Ethernet of USB). Uiteraard zijn afspraken hoe een verbinding wordt opgebouwd en weer wordt afgesloten van belang. De fysieke laag kan soms meerdere bits tegelijk versturen over meerdere fysieke communicatiekanalen (bijvoorbeeld bij communicatie via een parallelle printerpoort) en kan helemaal van een tasbaar medium afzien, zoals bij een infraroodverbinding of een draadloze verbinding (via bijvoorbeeld Bluetooth of Wifi).

2.1.2 De datalinklaag

De datalinklaag houdt zich bezig met het versturen van *frames* (samenhangende en betekenisvolle groepjes bits) tussen systemen. Door het groeperen van bits in frames en het toevoegen van controlebits is het mogelijk om de functie van de fysieke abstractielaag uit te breiden. De fysieke laag verstuurt slechts afzonderlijke bits, zonder garantie voor een juiste ontvangst van deze bits. Door de datalinklaag worden problemen, zoals het niet aankomen van frames, het dubbel ontvangen van frames of het ontvangen van beschadigde frames, opgelost. Zo kan de volgende en hogere abstractielaag (de netwerklaag) er op vertrouwen dat de verbinding de volledigheid en juistheid van het datatransport waarborgt.

De datalinklaag gaat uit van de specificaties in de opbouw van een frame (hoeveel startbits en in welk patroon, hoeveel databits, hoeveel stopbits en in welk patroon?) en van de timing tussen frames. Als hierbij fouten

optreden wordt er vaak gesproken van *framing errors*. Deze framing errors kunnen veroorzaakt worden door een zender die te snel achter elkaar frames verstuurt of door een zender die probeert te grote frames te versturen. De abstractielaag maakt gebruik van een parameter die MTU (Maximum Transmission Unit) heet en die aangeeft hoeveel data er maximaal in één frame mag zitten. Een voorbeeld hiervan is het Media Access Protocol (MAC-protocol) dat dergelijke afspraken in detail beschrijft.

Veel netwerkcomponenten (waaronder firewalls) maken gebruik van de informatie van deze abstractielaag om het netwerkverkeer te regelen en netwerkpakketten te filteren. Een voorbeeld zijn de zogenaamde *layer 2-switches* die vaak vele interfaces (zestien of meer) hebben waartussen zij dataverkeer schakelen. De switches gebruiken het MAC-adres van de aangesloten systemen om te besluiten welk verkeer via welke interface (al dan niet) verzonden moet worden.

2.1.3 De netwerklaag

De netwerklaag houdt zich bezig met het versturen van *pakketten* tussen systemen. Waar de voorafgaande abstractielaag een foutvrije verbinding tussen twee punten aanbiedt, is deze netwerklaag verantwoordelijk voor het juist routeren van netwerkpakketten over de vele mogelijke netwerkpaden tussen zender en ontvanger (waarbij één netwerkpad over tientallen tussenliggende systemen kan lopen). De netwerklaag verzorgt ook de snelheidsregeling van de datacommunicatie (zodat er tussen een snelle zender en een langzame ontvanger geen pakketten verloren gaan) en administreert de hoeveelheid data die verstuurd is (om dit te kunnen doorberekenen aan gebruikers van het netwerk).

Deze abstractielaag wordt bij TCP/IP door het Internet Protocol (IP) ingevuld. Veel netwerkcomponenten (waaronder firewalls) maken gebruik van informatie van deze abstractielaag. Een voorbeeld zijn de zogenaamde *layer 3-switches* die het IP-adres gebruiken om te besluiten welk verkeer via welke interface (al dan niet) verzonden moet worden.

2.1.4 De transportlaag

De transportlaag houdt zich bezig met het versturen van *berichten* tussen systemen. Waar de voorafgaande abstractielaag een foutvrije verbinding en een correcte routering aanbiedt, zorgt deze abstractielaag voor het opbreken van te grote berichten in kleinere pakketten die makkelijker verstuurd kunnen worden. Ook zorgt de abstractielaag ervoor dat de juiste berichten naar de juiste geadresseerden gaan (dit kan betekenen dat er meerdere verbindingen naar meerdere computers moeten worden bijgehouden).

Een verschil met de vorige en lagere abstractielagen is dat deze abstractielaag een tijdelijke, maar betrouwbare verbinding opbouwt met het eindpunt (de geadresseerde) en daarbij geen aandacht (meer) hoeft te besteden aan alle tussenliggende systemen (vergelijkbaar met een telefoongesprek, waarbij de tussenliggende elektronica volledig transparant is).

Deze abstractielaag (4) wordt meestal in het besturingssysteem van een computer geïmplementeerd en communiceert met abstractielaag 3 (netwerk) die geïmplementeerd als een *device driver* voor de netwerkkaart van de computer. De voorafgaande abstractielagen 2 en 1 zijn meestal in de netwerkkaart ingebouwd als firmware (programmeerbare schakeling) en hardware (niet-programmeerbare chip).

De transportlaag wordt bij TCP/IP door het Transmission Control Protocol (TCP) ingevuld. Bijna alle firewalls en de zogenaamde *layer 4-5-6-switches* gebruiken informatie binnen het TCP-protocol om te besluiten welk dataverkeer op welke interface moet worden doorgelaten of geblokkeerd.

2.1.5 De sessielaag

De sessielaag houdt zich net als de transportlaag bezig met het versturen van *berichten* tussen systemen, maar daarbij ook met het opzetten en onderhouden van een verbinding tussen zender en ontvanger. Nadat de verbinding is opgezet verzorgt de sessielaag het gebruik van deze verbinding door de eindgebruiker.

Belangrijke functies van deze abstractielaag zijn:
- de afstemming tussen zender en ontvanger van wie er gebruik mag maken van de verbinding (authenticatie, autorisatie en het bijhouden van gegevens voor facturering);
- de afstemming tussen zender en ontvanger van welke specifieke opties gebruikt gaan worden (bijvoorbeeld time-outwaarden van de verbinding);
- de afstemming tussen zender en ontvanger van het synchroniseren van meerdere verbindingen of berichten zodat voor de hogere abstractielagen (en uiteindelijk voor de gebruiker) de schijn wordt gewekt dat er slechts één betrouwbaar communicatiekanaal is.

Met betrekking tot het laatste punt het volgende. Het is mogelijk dat voor één bepaalde transactie tussen computer A en computer B een grote verzameling van samengestelde berichten en deelberichten nodig is, die via verschillende netwerkprotocollen naar weer andere computers gaan. Het is mogelijk dat de resultaten van de verschillende berichten eerst gecombineerd moeten worden voordat ze naar de hogere lagen kunnen worden doorgegeven. Dit komt vooral bij transactieverwerkende systemen voor.

Het komt voor dat de sessielaag geïntegreerd is met de transportlaag of zelfs niet aanwezig is. Het is niet gebruikelijk dat firewalls informatie uit deze abstractielaag gebruiken voor de sturing van het dataverkeer. Dit komt doordat op deze laag vaak zeer specifieke informatie aanwezig is, die alleen in de juiste en vaak complexe context juist geïnterpreteerd kan worden. Dat kan bijvoorbeeld wel in de speciaal hiervoor ontwikkelde betalingsverkeerprogrammatuur, maar niet in de algemeen toepasbare netwerkcomponenten zoals routers en firewalls.

2.1.6 De presentatielaag

De presentatielaag houdt zich bezig met het op de juiste manier weergeven van informatie. Dit is nodig omdat verschillende computersystemen verschillende manieren gebruiken om dezelfde informatie te representeren. Het traditionele voorbeeld hiervan is het verschil tussen de ASCII- en de EBCDIC-karaktersets. Voor een zinvolle communicatie tussen twee van dergelijke systemen moet er eerst conversie plaatsvinden.

Een meer actueel voorbeeld is het gebruik van geïntegreerde encryptiesoftware die, transparant voor de gebruiker, leesbare tekst versleutelt naar gecodeerde tekst voordat die verstuurd wordt. Aan de ontvangende kant moet de gecodeerde informatie weer automatisch en transparant ontsleuteld worden.

De beschikbare informatie en functionaliteit op deze abstractielaag worden zelden gebruikt door netwerkcomponenten, filters en firewalls. Dit komt ook doordat de afbakening tussen de abstractielagen 5, 6 en 7 (sessie, presentatie en applicatie) vaak zeer vaag is.

Op deze hogere lagen heeft het ISO-OSI-model slechts een zwakke relatie met de praktijk van netwerken en systemen. Het gebruik van het model op deze lagen wordt al gauw abstract en theoretisch en sluit niet goed aan op de implementaties die in de praktijk zijn ontwikkeld.

2.1.7 De applicatielaag

De applicatielaag zorgt voor de interactie met de gebruiker (of met een andere applicatie) en voor de juiste aansturing van de lagere abstractielagen. In de applicatielaag wordt bepaald of er netwerkverkeer nodig is en hoe dat netwerkverkeer geïnitieerd moet worden.

De beschikbare informatie en functionaliteit op deze abstractielaag is zeer krachtig en wordt vaak gebruikt door zogenoemde *application level firewalls*. Deze firewalls (ook proxy's genoemd) kunnen de inhoud en de (technische) bedoeling van de datacommunicatie interpreteren en op basis hiervan dataverkeer doorlaten of blokkeren. Een voorbeeld hiervan is dat vanuit dezelfde applicatie leesopdrachten wél worden toegestaan (bijvoorbeeld een 'GET'-opdracht binnen een FTP-communicatiesessie) terwijl schrijfopdrachten níet worden toegestaan (bijvoorbeeld een 'PUT'-opdracht binnen dezelfde FTP-communicatiesessie).

Bovendien is het op deze abstractielaag mogelijk om beschikbare contextgegevens (zoals servernamen, applicatienamen, gebruikersnamen, tijdstippen en locatiecodes) te betrekken in het beslissingsproces.

Ten slotte moet hier worden opgemerkt dat op de hogere lagen het verband tussen de theorie van het ISO-OSI-model en de praktijk niet optimaal is, zodat het model soms meer verwarring dan helderheid schept. Theorie en praktijk sluiten het best op elkaar aan op de lagen 1 (fysieke laag), 2 (datalinklaag), 3 (netwerklaag), 4 (transportlaag) en 7 (applicatielaag).

2.1.8 Voor- en nadelen van abstractielagen

De grootste kracht van het ISO-OSI-model is dat de functionaliteit en de complexiteit van de communicatie in een aantal abstractielagen zijn opgedeeld. Dit maakt het ontwerp en de realisatie van de functies voor gegevensuitwisseling gemakkelijker. Functies kunnen binnen één laag volledig anders gerealiseerd worden en er kunnen functies worden toegevoegd of verwijderd, zolang de interfaces tussen de abstractielagen maar gelijk blijven. Het maakt bijvoorbeeld voor de interfaces nauwelijks verschil of een abstractielaag in software of in hardware gerealiseerd wordt.

Een nadeel van het opdelen in verschillende abstractielagen is het vergroten van de *overhead*. Bij elke doorgifte van gegevens tussen abstractielagen moet (theoretisch gezien) steeds een kopie van de gegevens worden gemaakt. Nadat de gegevens zijn doorgegeven moeten deze kopieën weer worden gewist en moet de gebruikte geheugenruimte weer worden vrijgegeven. Dit brengt in de praktijk veel kopieeracties met zich mee, die vooral op oudere systemen tot performanceproblemen leiden.

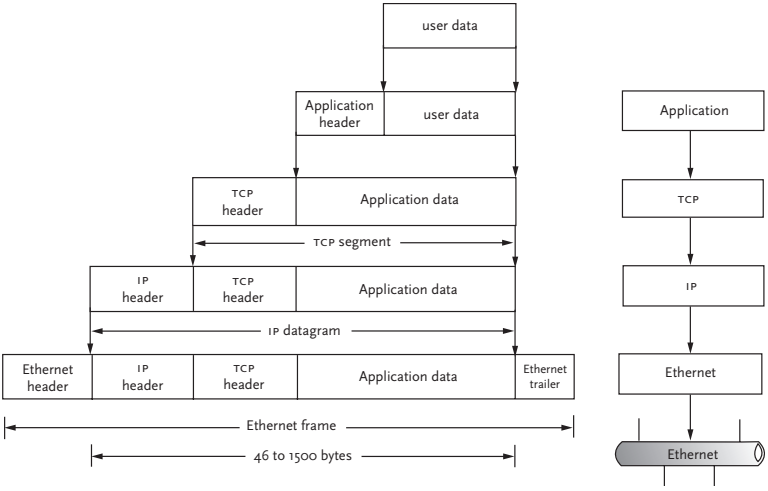
Er zijn veel implementaties op de markt gebracht die zich niet hielden aan de scheiding van abstractielagen en die de gegevens niet netjes doorgaven en kopieerden van abstractielaag naar abstractielaag, maar die bijvoorbeeld één kopie door alle abstractielagen lieten gebruiken en wijzigen. Het gevolg hiervan was dat er weliswaar een performanceverbetering optrad, maar tegelijk ook een verslechtering op het gebied van uitwisselbaarheid en stabiliteit van de software.

De verwerkingssnelheid van moderne computers is zo groot, dat de extra belasting door het kopiëren, inpakken en uitpakken van gegevens geen

probleem meer zou moeten zijn. Maar met de toename van de verwerkingssnelheid nemen ook de bandbreedtes en de hoeveelheden data toe. Een voorbeeld hiervan is het gebruik van Gigabit Ethernet voor de netwerktoegang van werkstations, waarbij tegelijkertijd grote hoeveelheden beeld, geluid, telefonie en gegevens via het netwerk naar de computer gaan. Hierdoor is het ontwikkelen van software, die het maximale uit de beschikbare apparatuur, programmatuur en netwerk haalt, nog steeds iets voor vakmensen.

2.1.9 *Encapsulatie: inpakken en uitpakken*

Zoals eerder aangegeven worden de te verzenden gegevens doorgegeven van abstractielaag naar abstractielaag, totdat zij op laag 1 uitkomen en dan via het fysieke medium worden verzonden. Elke abstractielaag voegt extra (hulp)gegevens toe, die zij nodig heeft om de gegevens correct te kunnen verwerken. Zie figuur 2.2.



Figuur 2.2 Encapsulatie: de stappen

Het toevoegen van informatie op de bepaalde abstractielagen heet 'encapsulatie'. Encapsulatie wordt op alle lagen in bepaalde mate gedaan

en is afhankelijk van het gebruikte netwerkprotocol. In het TCP/IP-protocol wordt bijvoorbeeld op de transportlaag een *TCP-header* voor de data geplaatst. Dit pakket wordt vervolgens doorgegeven aan de netwerklaag die er een *IP-header* voor plaatst. Sommige protocollen voegen behalve een header ook een trailer aan de informatie toe voordat ze de informatie doorgeven naar de volgende abstractielaag.

Figuur 2.3 is een voorbeeld van encapsulatie. De te verzenden gegevens (data) worden via het TCP-protocol voorzien van een TCP-header en doorgegeven aan het IP-protocol. Het IP-protocol voegt aan het begin van het pakket een IP-header toe. Uiteindelijk zal het pakket via Ethernet verstuurd worden (waarbij het Ethernet-protocol voorschrijft dat er zowel een header voor het pakket als een trailer achter het pakket toegevoegd moet worden).

Figuur 2.3 Encapsulatie: het resultaat

Het 'uitpakken' van een ontvangen hoeveelheid gegevens loopt vanaf de onderste abstractielaag van het OSI-model naar boven. Eerst komt men informatie tegen van de fysieke laag, daarna van de datalinklaag (in dit voorbeeld Ethernet). Uiteindelijk worden de oorspronkelijke gegevens (data) uitgepakt en doorgegeven aan de applicatie of gebruiker.

De mate van overhead wordt in sterke mate bepaald door de totale hoeveelheid gegevens die verstuurd moet worden. Als de hoeveelheid gegevens te groot is om in een keer te versturen, dan worden de gegevens gesplitst in kleinere brokken, met de maximaal toegestane grootte (zie MTU in 2.1.2). De ongunstigste situatie (in termen van overhead) wordt bereikt als er slechts één bit verstuurd moet worden. In dat geval is de hoeveelheid gegevens in headers en trailers (de overhead) vele malen groter dan de hoeveelheid 'echte' informatie waar de gebruiker of applicatie in geïnteresseerd is.

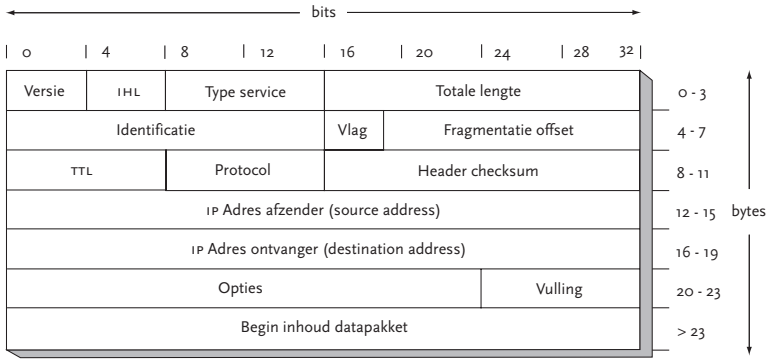
In paragraaf 2.2 over TCP/IP zullen de TCP-header en de IP-header uitvoerig besproken worden, omdat veel netwerkcomponenten, filters en firewalls hun beslissingen op de inhoud van deze headers baseren.

2.2 Het IP- en TCP-protocol

In deze studie wordt vooral ingegaan op het TCP/IP-protocol. Nauwkeuriger gezegd is dit het Internet Protocol versie 4 (IPv4) met het bijbehorende Transmission Control Protocol (TCP). Daarnaast wordt ook ingegaan op het User Datagram Protocol (UDP-protocol) en het Internet Control Message Protocol (ICMP-protocol), die beide gebruikmaken van het IP-protocol.

2.2.1 *Het IP-protocol*

Het IP-protocol is een zogenaamd *best-effort protocol*. Als het protocol een hoeveelheid gegevens moet verzenden, dan doet het daartoe één poging en gaat het er vervolgens vanuit dat de gegevens zijn aangekomen. Het protocol controleert niet of er onderweg naar de ontvanger problemen zijn opgetreden. De gegevens worden voorzien van een IP-header waarin gegevens over de zender en de ontvanger zijn opgenomen (te vergelijken met een envelop om een brief). De IP-header wordt door elk systeem op het netwerkpad van zender naar ontvanger gelezen. Als het systeem de IP-header leest en ontdekt dat het zélf de ontvanger is, dan verwerkt het de gegevens. Als het ontdekt dat het níet de bedoelde ontvanger is, dan worden de gegevens genegeerd. Figuur 2.4 toont de opbouw van de IP-header.



Figuur 2.4 IP-header

De velden van de IP-header hebben de volgende waarde en betekenis:

- Versie: bij IP-versie 4 heeft dit veld de waarde 4.
- IHL (IP-pakket-headerlengte): dit is de lengte van de IP-header in veelvouden van 32 bits.
- Type service: staat bekend als *differentiated service code point* (DSCP), dit veld heeft vaak de waarde 0 maar kan gebruikt worden om verschillende kwaliteitstypen aan te geven.
- Totale lengte: dit is de lengte van de IP-header en de data samen, uitgedrukt in veelvouden van acht bits (*bytes*).
- Identificatie: dit volgnummer wordt samen met het adres van de afzender gebruikt om gegevens die tijdens het transport in kleinere stukken zijn opgedeeld (fragmentatie), weer in de juiste volgorde samen te stellen.
- Vlag: bestaat uit drie bits die onder andere aangeven of een pakket tijdens het transport in kleinere stukken (fragmenten) opgedeeld mag worden of niet (in het Engels: *don't fragment* [DF]).
- Fragmentatie-offset: als een pakket onderdeel is van een groter pakket dat tijdens het transport is opgedeeld, dan geeft dit veld zijn positie aan binnen het oorspronkelijke (grotere) pakket. Deze informatie wordt gebruikt om het oorspronkelijke pakket weer samen te stellen met de fragmenten.
- *Time to live* (TTL): dit is het maximaal aantal keren dat het pakket doorgegeven mag worden. De teller wordt telkens met één verlaagd totdat de waarde nul bereikt is, waarna het pakket weggegooid wordt (zodat het niet oneindig in een netwerk blijft rondzwerven).
- Protocol: dit veld geeft aan bij welke transportlaag het pakket hoort in de encapsulatie (voorbeelden hiervan zijn de waarden 1: ICMP, 2: IGMP, 6: TCP en 17: UDP).
- *Header checksum*: dit controletotaal detecteert of er fouten zijn opgetreden in een van de andere velden. Als dit het geval is wordt het pakket weggegooid.
- IP-adres afzender: deze 32 bits vormen het IP-adres van de afzender.
- IP-adres ontvanger: deze 32 bits vormen het IP-adres van de ontvanger.
- Opties: in dit veld kunnen opties meegestuurd worden (wordt zelden gebruikt).
- Vulling: dit aantal bits zorgt ervoor dat de data met een veelvoud van 32 bits beginnen (in het Engels: *padding*).

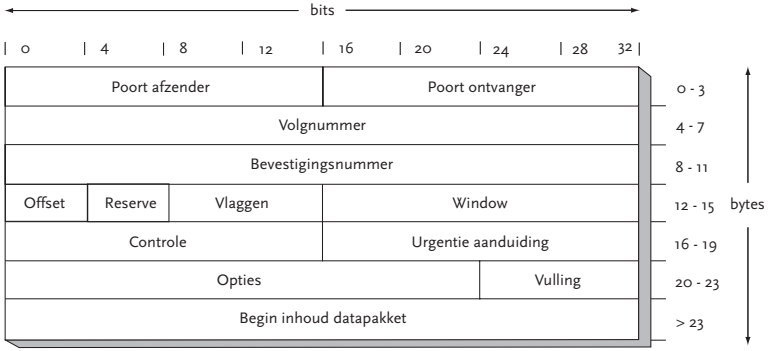
2.2.2 Het TCP-protocol

Het TCP-protocol is een zogenaamd *reliable* protocol. Het garandeert dat alle door het IP-protocol verstuurde pakketten in de goede volgorde bij de ontvanger afgeleverd worden. Het protocol houdt bij welke pakketten verstuurd zijn en blijft de pakketten versturen totdat het een ontvangstbevestiging ontvangt.

Een TCP-verbinding is, in tegenstelling tot de IP-verbinding, virtueel. Dit houdt in dat alleen de zender en de ontvanger de TCP-pakketten zien, alle tussenliggende systemen zien het IP-pakket. Voor de virtuele verbinding is het noodzakelijk dat er eerst een IP-verbinding wordt opgebouwd. De virtuele verbinding blijft in stand totdat deze expliciet wordt beëindigd. De opbouw van de TCP-verbinding, de zogenaamde *three-way handshake*, is zeer belangrijk en wordt in paragraaf 2.2.5 beschreven.

Figuur 2.5 toont de opbouw van de TCP-header. De velden van de TCP-header hebben de volgende waarde en betekenis:

– Poort afzender: een waarde die aangeeft welke service of applicatie de afzender vertegenwoordigde (bijvoorbeeld 20,21: FTP-service voor gegevenstransport, 23: TELNET-service voor remote login, 80: HTTP-service voor webbrowsing);
– Poort ontvanger: een waarde die aangeeft welke service of applicatie de gegevens moet ontvangen en verwerken;



Figuur 2.5 TCP-header

- Volgnummer: het volg- of identificatienummer van het huidige TCP-pakket;
- Bevestigingsnummer: het volg- of identificatienummer dat de ontvanger van de zender verwacht;
- Offset: geeft aan waar, ten opzichte van het begin van het TCP-pakket, de gegevens beginnen (deze waarde is minimaal 5);
- Gereserveerd: 4 bits met de waarde 0;
- Vlaggen: 8 bits waarvan er 6 gebruikt worden en die de volgende namen of afkortingen hebben: URG/ACK/PSH/RST/SYN/FIN. Deze besturen de gegevensuitwisseling;
- Window: geeft aan welke hoeveelheid data in één keer ontvangen kan worden;
- Controle: een checksum ter controle van de inhoud van het TCP-pakket;
- Urgentie-aanduiding: wijst naar het einde van de urgentedata (zie ook het veld 'vlaggen');
- Opties: extra data die gestuurd kan worden als de SYN-vlag gebruikt wordt. Dit bestuurt de gegevensuitwisseling;
- Vulling: aantal bits om ervoor te zorgen dat de data op een veelvoud van 32 bits begint (in het Engels: '*padding*').

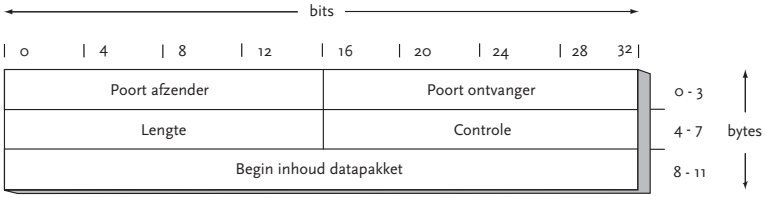
2.2.3 Het UDP-protocol

Voor de volledigheid wordt in deze paragraaf de UDP-header beschreven. Naast TCP is UDP (net als ICMP) een veelgebruikt transportlaagprotocol. Het UDP-protocol is unreliable omdat het geen garantie geeft of en hoe vaak het pakket bij de bedoelde ontvanger aankomt. In tegenstelling tot TCP hoeft niet eerst een virtuele verbinding opgebouwd te worden. Door zijn eenvoud is het UDP-protocol uitermate geschikt voor situaties waarbij de overhead van het TCP-protocol niet nodig (zoals bij *instant messaging*) of zelfs ongewenst is (zoals bij snelle computergames). Figuur 2.6 toont de opbouw van de UDP-header.

De velden van de UDP-header hebben de volgende waarde en betekenis:

- Poort afzender: de service/applicatie aan de zenderkant die dit pakket verstuurd heeft;

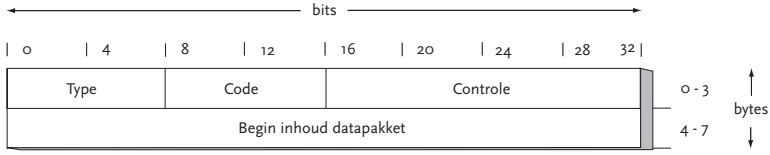
– Poort ontvanger: de service aan de ontvangerkant die dit pakket zou moeten verwerken;
– Lengte: de totale lengte van de UDP-header en de data;
– Controle: een optionele waarde die gebruikt kan worden voor het detecteren van fouten in de gegevens.



Figuur 2.6 UDP-header

2.2.4 Het ICMP-protocol

Het ICMP-protocol (de netwerklaag) wordt vooral gebruikt voor aansturing en controle van de juiste werking van de netwerkapparatuur. Het ICMP-pakket is nog eenvoudiger van opzet dan het UDP-pakket. Figuur 2.7 toont de opbouw van de ICMP-header.



Figuur 2.7 ICMP-header

Wat opvalt aan de opbouw van de ICMP-header is dat er geen apart adresveld aanwezig is. Het typeveld geeft aan welk controlemechanisme wordt gebruikt. De IP-header bevat zowel het adres van de ontvanger als van diegene die het antwoord wil terugontvangen (dit staat in het zenderveld). Het controleveld is de bekende checksum, die controleert of de inhoud van het pakket niet beschadigd is. De inhoud van het datagedeelte is afhankelijk van het gebruikte type, de eventueel bijbehorende code en het resultaat daarvan.

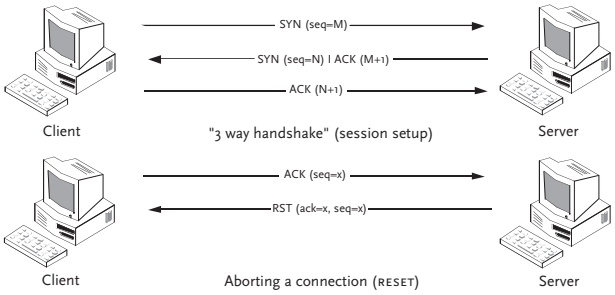
Op dit moment zijn er dertig verschillende soorten ICMP-berichten gedefinieerd waarvan de volgende het bekendst zijn:

– Type 8 en type 0: de zender zendt een type 8 ICMP-bericht naar de ontvanger, die geacht wordt te antwoorden met een type 0 ICMP-bericht. Dat wil zeggen dat de zender een *echo* ICMP-bericht stuurt, waarop de ontvanger een *echo reply* zou moeten terugsturen. Deze volgorde staat bekend als 'ping'. Hierdoor wordt nagegaan of twee systemen met elkaar kunnen communiceren.
– Type 3: het *destination unreachable* ICMP-bericht. Dit is een goed voorbeeld van een type ICMP-bericht dat ook het codeveld gebruikt. Het typeveld geeft aan dat er problemen zijn (de bedoelde ontvanger kan niet bereikt worden), het codeveld geeft aan wat de oorzaak van de problemen is (bij dit type zijn er zestien codes gedefinieerd).

In deze firewall-studie ligt de nadruk op de combinatie van IP- en TCP-pakketten. Indien relevant, wordt expliciet aangegeven wat de verschillen zijn ten opzichte van de UDP- en ICMP-pakketten.

2.2.5 De opbouw van een TCP-verbinding

Het belangrijkste onderdeel van de TCP-communicatie is het opzetten van de virtuele verbinding tussen zender en ontvanger. Hiertoe wordt in een vaste volgorde een aantal pakketten uitgewisseld tussen zender en ontvanger. Dit staat bekend als een 'three-way handshake', die aan de hand van figuur 2.8 wordt besproken.



Figuur 2.8 Three-way handshake

In dit voorbeeld wil de client (A, links) een verbinding opzetten met de server (B, rechts). Daarvoor stuurt de client een TCP-pakket waarin de SYN-vlag op 1 staat en de overige vlaggen op 0 staan (SYN staat voor 'synchroniseer', zie ook paragraaf 2.2.2). Dit is de eerste en meest essentiële stap om een TCP-verbinding op te zetten. Als de firewall alle pakketten zou tegenhouden waarin de SYN-vlag aanstaat, dan zou er geen TCP-communicatie mogelijk zijn.

> Stap 1 is dus: de client (A) stuurt een TCP-pakket met de SYN-vlag op 1 naar de server (B).

Na het succesvol ontvangen door de server (B) van het TCP-pakket met de SYN-vlag, wordt er besloten dat de server (B) de verbinding tot stand wil brengen met de client (A) die het pakket gestuurd heeft. De server (B) stuurt dan een TCP-pakket terug naar de client (A) waarin de SYN- en de ACK-vlaggen op 1 zijn gezet (ACK staat voor 'acknowledge' en geeft aan dat de verbinding tot stand mag worden gebracht).

> Stap 2 is dus: de ontvanger (B) stuurt een TCP-pakket met een SYN- en een ACK-vlag terug naar de client (A).

Nadat client A het TCP-pakket 'SYN + ACK' (afkomstig van server (B)) heeft ontvangen, stuurt client (A) een TCP-pakket met een ACK-vlag terug naar server (B). Hiermee is de derde stap afgerond en is de virtuele TCP-verbinding totstandgekomen.

> Stap 3 is dus: client (A) stuurt een TCP-pakket met de ACK-vlag terug naar server (B).

Na het succesvol totstandkomen van de virtuele verbinding zullen alle volgende TCP-pakketten de ACK-vlag op 1 hebben gezet. Dit is onder andere waarom het belangrijk is de status van de verbinding bij te houden. Indien een firewall een TCP-pakket ontvangt met de ACK-vlag aan, betekent dit dan dat het pakket onderdeel is van een legitieme en al bestaande virtuele verbinding of niet? Om dit probleem op te lossen zijn er zogenaamde *stateful* firewalls die een boekhouding bijhouden van alle actieve verbindingen (zie paragraaf 4.2.2).

Naast het opbouwen van een virtuele TCP-verbinding is ook het afbreken van een virtuele TCP-verbinding gebonden aan een specifiek protocol. Dit protocol wordt aangeduid als de *four-way handshake* en werkt als volgt:

- Stap 1: systeem A stuurt systeem B een pakket met het verzoek de verbinding af te breken. Het betreft een TCP-pakket met de ACK- en FIN-vlaggen (FIN staat voor *finish*).
- Stap 2: systeem B antwoordt door middel van een TCP-pakket met de ACK-vlag aan.
- Stap 3: systeem B stuurt dan op zijn beurt een pakket naar systeem A met het verzoek de verbinding af te breken. Het betreft een TCP-pakket met de ACK- en FIN-vlaggen.
- Stap 4: systeem A antwoordt door middel van een TCP-pakket met de ACK-vlag aan.

De eerste twee stappen verbreken de verbinding van A naar B, de laatste twee stappen verbreken de verbinding van B naar A.

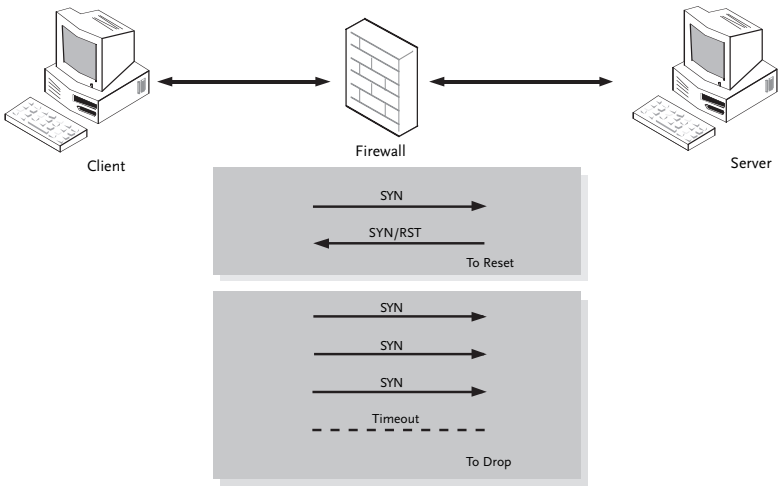
Een andere manier om een virtuele TCP-verbinding te verbreken is het sturen van een TCP-pakket met de RST-vlag (RST staat voor *reset*) op 1. Dit TCP-pakket kan verstuurd worden als onderdeel van een normale verbinding (en dan zal ook de ACK-vlag op 1 gezet zijn), maar ook zonder onderdeel te zijn van een verbinding (en dan zal er ook geen ACK-vlag zijn). Dit zal een onmiddellijke verbreking van de virtuele TCP-verbinding veroorzaken, zonder dat er TCP-pakketten met de ACK-vlag op 1 gestuurd worden.

De hierboven beschreven combinaties zijn zo bedoeld door de ontwerpers van het TCP-protocol. In de praktijk zijn echter ook allerlei andere combinaties van TCP-vlaggen mogelijk, zoals een TCP-pakket met zowel de SYN- als de FIN-vlag. Deze combinatie is niet logisch en kan ook niet voorkomen bij normaal gebruik van het TCP-protocol. Deze en andere afwijkende combinaties van TCP-vlaggen kunnen een teken van misbruik zijn; iets of iemand probeert misbruik te maken van netwerksystemen.

Omdat deze combinaties normaalgesproken niet voorkomen, houden veel TCP-implementaties er geen rekening mee. Als dan toch een dergelijk 'onmogelijke' combinatie voorkomt, dan weet de programmatuur vaak niet hoe zij hier op moet reageren. In het minst erge geval gebeurt

er niets. Er zou een foutmelding gegenereerd moeten worden en de verbinding die de fout veroorzaakt, zou verbroken moeten worden. Soms reageert de programmatuur verkeerd en loopt het systeem vast of er ontstaat een onvoorspelbare situatie waarin het systeem extra kwetsbaar wordt voor verdere aanvallen.

Een firewall zal in het algemeen ongewenste verbindingen verbreken of weigeren. De officiële werkwijze is het versturen van een TCP-pakket met de FIN- en ACK-vlaggen of een TCP-pakket met de RST-vlag (en de ACK-vlag). Hierdoor weet het andere systeem dat de verbinding verbroken wordt. Het gaat dus om communicatie naar het andere systeem toe en dat kan gevolgen hebben. Als het andere systeem 'vijandig' is, dan kan de communicatie misbruikt worden bij het opzetten van nieuwe aanvallen. Zo is het bijvoorbeeld mogelijk om te achterhalen welke applicaties/services actief zijn. Deze onnodige 'informatielekkage' kan voorkomen worden door de 'vijandige' TCP-pakketten te negeren (in het Engels: *to drop*). Dit vraagt ook minder performance van de firewall. Een regelmatig gestelde vraag bij firewalls is dan ook: '*To drop or to reset?*', zie figuur 2.9.



Figuur 2.9 To drop or to reset?

3 Filteren van netwerkverkeer

In dit hoofdstuk wordt een aantal nieuwe begrippen geïntroduceerd. Deze zijn nodig voor een goed begrip van de hoofdstukken waarin de verschillende typen en verschijningsvormen van firewalls worden beschreven.

3.1 Definitie firewall

In deze paragraaf wordt beschreven wat er in deze studie met de term 'firewall' bedoeld wordt. Om te beginnen de definitie die in deze studie wordt gebruikt:

> *Een firewall is een combinatie van apparatuur en programmatuur waarbij het mogelijk is om, via opgestelde regels, netwerkverkeer te beheersen. Hierdoor kan netwerkverkeer tussen verschillende domeinen gereguleerd worden.*

Deze definitie van een firewall is met opzet niet te specifiek gemaakt omdat in de praktijk blijkt dat er veel manieren zijn om het bovenstaande te realiseren. In bovenstaande definitie behoeft de term 'domein' toelichting. De volgende omschrijving komt uit de publicatie *PI-Basisnormen Beveiliging en Beheer IT-Infrastructuur*:

> *Een domein van de IT-infrastructuur is de verzameling van alle clients, servers en de verbindingen hiertussen, die op netwerkniveau zonder enige beperking contact met elkaar kunnen opnemen en gegevens(-pakketten) kunnen uitwisselen.*

Domeinen kunnen op verschillende manieren aangewend worden. Voorbeelden daarvan zijn:

– intranet: gekoppelde domeinen binnen één organisatie(onderdeel);
– extranet: gekoppelde domeinen tussen verschillende, elkaar in meer of mindere mate vertrouwende (onderdelen van) organisaties of partners;
– internet: wereldwijde koppeling van domeinen tussen anonieme partijen die elkaar niet kunnen vertrouwen.

Naast deze voorbeelden zijn er nog legio andere praktijkvoorbeelden die het gebruik van domeinen en het scheiden van deze domeinen door een firewall rechtvaardigen.

Een firewall kan gerealiseerd worden met behulp van een standaardcomputer en firewall-software die de firewall-functionaliteit levert. Voorbeelden hiervan zijn bekende commerciële firewalls als Firewall-1 van CheckPoint en ISA Server van Microsoft. Een firewall kan ook gerealiseerd worden door een speciaal daarvoor ontwikkeld (hardware-)systeem. Voorbeelden hiervan zijn de PIX Firewall van Cisco en de apparatuur van Symantec. Firewalls worden tegenwoordig ook ingebouwd in andere netwerkapparatuur, zoals (ADSL-)routers. Ten slotte is het mogelijk om met een combinatie van componenten (routers, switches en computers) een firewall-concept te verwezenlijken. In hoofdstuk 5 over ontwerpcriteria zal dieper op de verschijningsvormen van firewalls worden ingegaan.

Naast functionaliteit en ontwerpcriteria is een zeer belangrijk, zo niet het belangrijkste, aspect van een firewall het beheer van de firewall. Hier valt niet alleen de initiële configuratie van een firewall onder, maar vooral ook het continu bijhouden van de zogenaamde *rule set* (de filterregels) en het monitoren van de logbestanden. Hoofdstuk 7 zal geheel aan firewall-beheer worden besteed.

3.2 Filteren van netwerkverkeer

In deze paragraaf wordt een overzicht gegeven van de redenen tot filtering, wat er precies gefilterd wordt, welke technieken hiervoor beschikbaar zijn en in hoeverre netwerkfilters van elkaar verschillen. De nadruk zal liggen op de technische achtergrond van het filteren. In latere hoofdstukken wordt ingegaan op de keuze van specifieke filters voor specifieke situaties.

3.2.1 Redenen tot filtering

De huidige versie van het TCP/IP-protocol stamt uit een tijd waarbij het samenwerken op en het delen van computersystemen gebruikelijk was. Er waren relatief weinig computersystemen beschikbaar, er was relatief weinig informatie op de systemen aanwezig en de meeste gebruikers kenden elkaar persoonlijk. De computersystemen werden vooral voor academische doeleinden gebruikt.

De laatste tien of twintig jaar is hier verandering in gekomen. Haast iedereen heeft één of meerdere computersystemen, er wordt met een grote verscheidenheid aan systemen gecommuniceerd en zeer veel (zeer gevoelige) informatie staat op systemen die via netwerken te bereiken zijn.

Helaas gaat de huidige versie van TCP/IP niet adequaat om met deze schaalvergroting en het veranderde gedrag van de netwerkgebruikers.

Dit heeft geleid tot het besef dat informatie en computersystemen beschermd moeten worden tegen al dan niet opzettelijk misbruik. Grotere risico's en een groeiend verantwoordelijkheidsgevoel hebben daaraan hun steentje bijgedragen, maar wet- en regelgeving heeft een aanjagend grote rol gespeeld. Het is zelfs mogelijk om korting te bedingen op abonnementskosten of verzekeringspremies als men kan aantonen dat voldoende beveiligingsmaatregelen getroffen zijn – waarbij netwerkfiltering een belangrijk aspect is.

De redenen tot filtering zijn dan ook legio, om er een aantal te noemen:
- lokale en landelijke wet- en regelgeving inzake gebruik computersystemen;
- bescherming privacygevoelige gegevens;
- bescherming bedrijfsgevoelige gegevens;
- bescherming en controle van computersystemen;
- bescherming tegen virussen en andere schadelijke zaken.

Naast de hierboven genoemde redenen zijn er ook netwerken die beschermd moeten worden tegen al dan niet opzettelijke verstoring van buitenaf. Hierbij kan gedacht worden aan infrastructuren zoals meldkamers van politie, brandweer en ambulances en ziekenhuizen, waar uitval van computersystemen levensbedreigende situaties kan veroorzaken.

3.2.2 Belangrijkste filtertechnieken

Er zijn verschillende typen firewalls op de markt. Een bruikbare indeling kan worden gemaakt op basis van het inspectiemechanisme, waarmee de firewall besluit om netwerkverkeer wel of niet door te laten.

Het volgende firewall-overzicht, gebaseerd op het toegepaste inspectiemechanisme, wordt in de volgende paragrafen van deze studie uitgewerkt:
- filter statisch per netwerkpakket (*static packet filter*);
- filter dynamisch per netwerkpakket (*dynamic [stateful] packet filter*);
- filter gebaseerd op netwerkverbindingen (*circuit level gateway*);
- filter gebaseerd op toegepaste applicatie (*application level gateway [proxy]*);
- filter gebaseerd op een combinatie van bovenstaande technieken (*hybrid inspection*);
- filter gebaseerd op snelheid (*cutoff proxy*);
- filter dat netwerken 'gescheiden' houdt (*air gap*).

Op alle typen filters zijn de volgende opmerkingen van toepassing:

Voordat de firewall een netwerkpakket doorstuurt, worden van elk netwerkpakket de IP- en TCP-headers (en soms additionele informatie) bekeken en wordt er gecontroleerd of bepaalde filterregels van toepassing zijn. Deze regels worden in het algemeen in tabelvorm opgeslagen (rule set). De regels van de tabel worden stuk voor stuk doorlopen en voor elke regel wordt nagegaan of zij van toepassing is op het betreffende netwerkpakket.

Als een regel van toepassing is, wordt de bijbehorende actie op het netwerkpakket toegepast. De actie kan bijvoorbeeld 'doorlaten', 'niet doorlaten' of 'loggen' zijn. Alle regels worden doorgelopen totdat er een regel wordt gevonden die van toepassing is of totdat er geen regels meer zijn. Deze procedure wordt voor elk netwerkpakket uitgevoerd en bij een toenemend aantal regels zal ook de verwerkingstijd per netwerkpakket toenemen.

Er zijn twee opvattingen over wat te doen als er géén regel wordt gevonden die van toepassing is op het netwerkpakket, te weten:

- Toestaan: deze keuze leidt tot het beleid 'alles mag, tenzij het expliciet wordt verboden'. Als er geen enkele regel wordt gespecificeerd is dus alles toegestaan.
  Dit heet in het Engels *implicit allow all* en wordt vaak in omgevingen toegepast met een reactief beleid op het gebied van beveiliging. Alleen als netwerkverkeer 'last' veroorzaakt, wordt een regel toegevoegd die het hinderlijke verschijnsel tegenhoudt bij de firewall.
- Niet toestaan: deze keuze leidt tot het beleid 'niets mag, tenzij het expliciet wordt toegestaan'. Als er geen enkele regel wordt gespecificeerd mag dus niets. Dit heet in het Engels *implicit deny all* en wordt vaak in omgevingen toegepast met een actief beleid op het gebied van beveiliging. Alleen als er aangetoond is dat het netwerkverkeer geen gevaar oplevert, wordt er een regel toegevoegd zodat het niet langer door de firewall wordt tegengehouden.

Uiteraard kan er altijd als laatste regel in de tabel een regel worden opgenomen die expliciet alles toestaat of expliciet alles verbiedt.

De systeembeheerder kan in de tabel met regels specificeren welke netwerkpakketten geselecteerd worden voor welke acties. Hiervoor worden zowel de IP-header als de TCP-header gebruikt. Via de IP-header kan één adres (van zender en/of ontvanger) worden geselecteerd, evenals hele adresgebieden. Met behulp van de TCP-header kunnen services/applicaties geselecteerd worden (die worden via de TCP-poortnummers aangegeven).

Met deze gegevens is het bijvoorbeeld mogelijk om het raadplegen van informatie (met bijvoorbeeld een webbrowser) vanaf een bepaalde computer wel toe te staan en vanaf alle andere computers niet. Een ander voorbeeld is het toestaan van bestandsuitwisseling tussen een beveiligde server (via het FTP-protocol) en een gelimiteerde reeks van clients.

De systeembeheerder kan ook een regel in de tabel opnemen, die al het verkeer van onbekende afzenders blokkeert. Deze regel maakt het voor een hacker moeilijker (maar nog niet op voorhand onmogelijk) om toegang tot bepaalde systemen te verkrijgen.

Het samenstellen van de tabel met regels is een moeilijk en complex proces. Hoewel het beslissingsproces per netwerkpakket relatief snel verloopt (er wordt namelijk maar een kleine hoeveelheid data in het beslissingsproces gebruikt), kan een teveel aan regels de verwerkingssnelheid gaan beïnvloeden. Bovendien is het foutloos samenstellen van een lange tabel met regels moeilijk. Zie paragraaf 6.4.

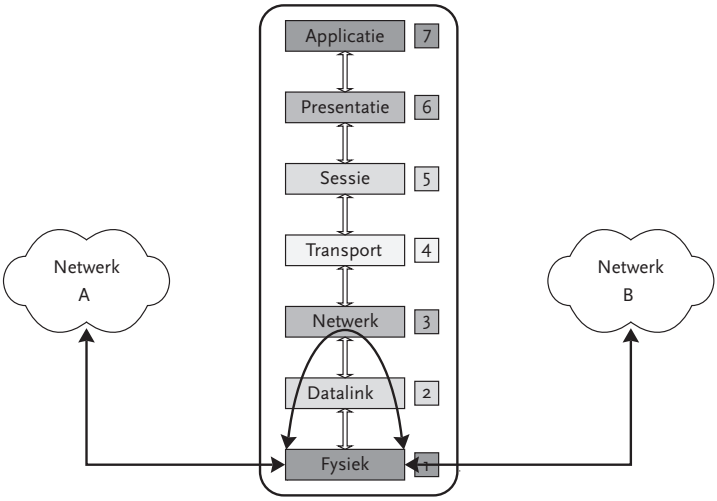
3.2.3 Statisch pakketfilter (static packet filter)

Zoals in het vorige hoofdstuk over TCP/IP beschreven is, hebben alle netwerkpakketten een standaardindeling. Aan het begin van deze netwerkpakketten (in de header) staat informatie (over onder meer afzender, geadresseerde en protocol) waarop firewalls hun beslissingen baseren.

Dit type firewall, het statische pakketfilter, is een van de oudste soorten firewalls die beschikbaar zijn. Een router die als firewall wordt ingezet zal in het algemeen ook als een statische filter werken – elk pakket wordt afzonderlijk bekeken. Er wordt niet gekeken naar relaties tussen opeen-

volgende pakketten. Andere voorbeelden van het gebruik van deze techniek zijn de oudere netwerkcomponenten van DLINK en LinkSys.

In relatie tot het ISO-model kan een statische pakketfilter zoals getoond in figuur 3.1 gepositioneerd worden.



Figuur 3.1 Statisch pakketfilter

Het mogelijke netwerkverkeer tussen netwerk A en netwerk B (ongeacht of dit nu interne of externe netwerken zijn) wordt bij dit type op ISO-laag 3, de netwerklaag, beoordeeld. Hier wordt de beslissing genomen om het verkeer wel of niet toe te staan.

Het beslissingsproces baseert zich op de volgende velden van de TCP/IP-headers:

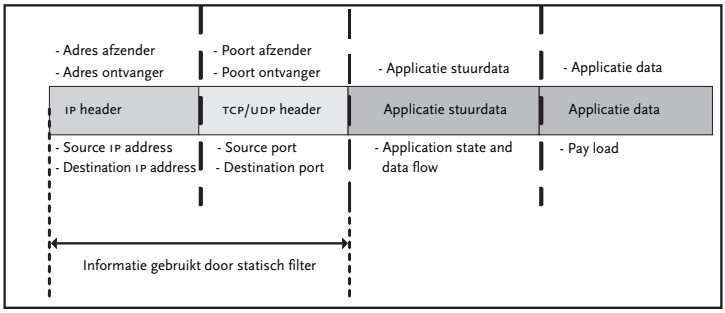
– adres zender (*source address*);
– adres ontvanger (*destination address*);
– gebruikt netwerkprotocol (*application or protocol*);
– verzendend programma (*source port number*);
– ontvangend programma (*destination port number*).

Zoals reeds vermeld maken de meeste bekende netwerkapplicaties en -functies gebruik van vaste en bekende netwerkpoorten (poortnummers). Enkele voorbeelden zijn:

– Poort 20 en 21: FTP, bestandsoverdracht
– Poort 25: SMTP, mailverzending
– Poort 80: HTTP, webbrowsing
– Poort 119: NNTP, raadplegen van nieuwsgroepen
– Poort 1521: Oracle database

De binding tussen een applicatie en een bepaald poortnummer is enigszins flexibel. Dit betekent dat Hyper Text Transfer Protocol (HTTP) bijvoorbeeld standaard op poortnummer 80 actief is, maar er kan ook een willekeurig andere poort gebruikt worden (zo wordt poortnummer 8080 vaak gebruikt). Wel is in de zogenaamde RFC-documenten afgesproken dat de eerste 1024 poortnummers gereserveerd zijn voor standaardapplicaties – maar dit wordt nergens afgedwongen!

Figuur 3.2 geeft grafisch weer op welke informatie van de netwerkpakketten het statische pakketfilter werkzaam is.



Figuur 3.2 Gebruikte informatie bij het statische pakketfilter

Een statisch pakketfilter betrekt alleen de gegevens van de IP- en TCP-headers in het beslissingsproces. Een dergelijk filter kan geen verschil maken tussen gemanipuleerde informatie en valide informatie. Als het adres en de protocolinformatie aan de criteria van een regel voldoen en de bijbeho-

rende actie is het toelaten van een dergelijk netwerkpakket, dan zal het netwerkpakket doorgelaten worden, ongeacht de validiteit van deze data.

Op die manier kan een hacker de adresgegevens in een pakket manipuleren, zodat het adres van de afzender overeenkomt met een 'vertrouwd' systeem. Dan zal het filter de pakketten doorlaten. Als er antwoord wordt gegeven op deze pakketten, dan zal de hacker dit antwoord niet ontvangen, ze gaan immers naar een vervalst afzenderadres. Dit hoeft echter geen probleem te zijn voor de hacker – de schade kan dan al aangericht zijn. Deze klasse van aanvallen (het vervalsen van identiteiten) wordt *spoofing* genoemd ('zich anders voordoen'). In bovenstaand voorbeeld spreken we dan ook van IP-adresspoofing.

Een IP-spoofingaanval kan uitermate effectief zijn wanneer slechts statische pakketfilters gebruikt worden. Het CERT Coordination Center (een internationale waarschuwingsdienst voor IT-risico's) ontvangt zeer veel rapporten over dit soort succesvolle aanvallen. Ondanks de relatief grote snelheid van een statisch pakketfilter is de uiteindelijke veiligheid onvoldoende om vasthoudende hackers buiten de deur te houden.

Afgezien van de informatie die een statisch netwerkpakketfilter wél betrekt in het beslissingsproces, is het ook belangrijk om vast te stellen wat een dergelijk filter níet onderzoekt. Aangezien alleen de adressen en poortnummers van de zender en ontvanger bekeken worden, worden de andere data in de headers en de eventuele schadelijke data in het pakket zelf dus niet bekeken. Hackers kunnen zodoende oneigenlijk gebruik maken van de minder bekende velden in de headers. Deze techniek wordt aangeduid met de term *covert channel attack*.

Ten slotte kan worden opgemerkt dat een statisch netwerkpakketfilter niet contextgevoelig is. Dit betekent dat elk netwerkpakket afzonderlijk wordt beoordeeld en dat er geen verbanden worden gelegd tussen bijvoorbeeld inkomend netwerkverkeer (een opdracht) en het bijbehorende uitgaande netwerkverkeer (de resultaten van deze opdracht).

Dit wordt vooral belangrijk bij filters die het deny-all-principe hanteren. Bij dit soort filters moet namelijk niet alleen het inkomende gedeelte

expliciet worden toegelaten (waaraan vaak wordt gedacht) maar ook het bijbehorende uitgaande gedeelte (en daar wordt vaak niet aan gedacht).

Een bijkomend probleem is dat sommige communicatieprogramma's geen gebruik maken van vaste, en dus vooraf bekende, poortnummers. De poortnummers worden tijdens de communicatie bepaald. Programma's als het File Transfer Protocol (FTP, bestandsuitwisseling) en SMTP (e-mail) gebruiken vaak dynamisch toegekende poortnummers om te communiceren. Deze poortnummers worden toegekend op het moment dat ze nodig zijn en zijn afhankelijk van de beschikbaarheid van nog niet gebruikte poortnummers. De mogelijke poortnummers kunnen een breed bereik beslaan. Het resultaat is dat het filter het hele mogelijke bereik van poortnummers moet openzetten, hetgeen ongewenst is.

Ter afsluiting van deze paragraaf laat tabel 3.1 de voor- en nadelen zien van statische pakketfilters:

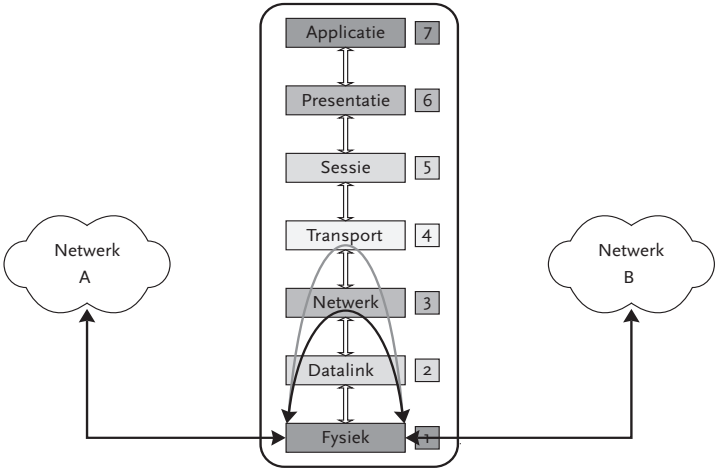
Tabel 3.1 Overzicht statisch pakketfilter

Overwegingen voor een statisch netwerkpakketfilter	
Voordelen	***Nadelen***
Relatief snel beslissingsproces per netwerkpakket	Werkt alleen op de netwerklaag en kijkt alleen naar een deel van de IP- en TCP-headers
Goedkoop en in ruime mate beschikbaar	Niet bewust van inhoud en data van netwerkpakketten, dit resulteert in beperkte beveiliging
	Niet contextgevoelig, veroorzaakt de noodzaak grote hoeveelheden adressen open te laten staan bij applicaties die dynamisch adressen gebruiken en toekennen
	Gevoelig voor spoofing
	Moeilijk om een effectieve, efficiënte en correcte set van regels te creëren bij complexere situaties
	Biedt een laag beveiligingsniveau

3.2.4 *Dynamisch pakketfilter (dynamic/stateful packet filter)*

Het dynamische pakketfilter staat op een hoger niveau in de ontwikkeling dan het statische pakketfilter. De overeenkomsten tussen deze twee filterversies, inclusief de voor- en nadelen, zijn dan ook zeer groot. Het meest essentiële verschil is dat het dynamische filter de toestand van de verbindingen administreert en mede daarop de beslissingen baseert (in het Engels: *state awareness*).

In relatie tot het ISO-model kan een dynamisch pakketfilter gepositioneerd worden zoals getoond in figuur 3.3.



Figuur 3.3 Dynamisch pakketfilter

Het dynamische pakketfilter werkt, net als het statische pakketfilter, vooral op OSI-laag 3, de netwerklaag. Sommige meer geavanceerde dynamische pakketfilters kunnen ook gebruik maken van statusinformatie van de OSI-laag 4, de transportlaag.

Het beslissingsproces richt zich op de volgende velden van de TCP/IP-headers:

– adres zender (source address);

– adres ontvanger (destination address);
– gebruikt protocol (application or protocol);
– verzendend programma (source port number);
– ontvangend programma (destination port number);
– opbouw, status en richting van de TCP-verbinding.

Een dynamisch pakketfilter weet of een netwerkpakket hoort bij een nieuwe of een bestaande netwerkverbinding en weet ook welk verkeer er als antwoord op een verzonden pakket terugverwacht kan worden.

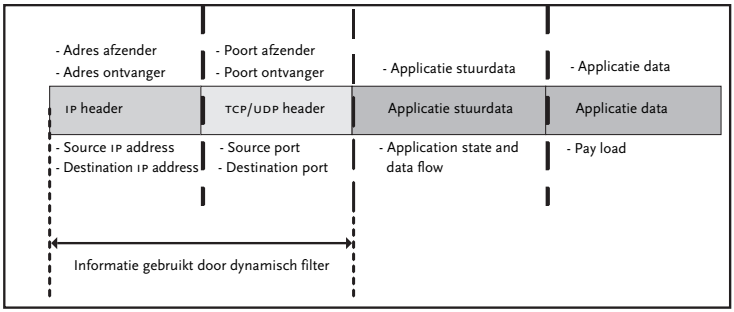
Als een verzoek voor een nieuwe verbinding geaccepteerd wordt en de verbinding opgebouwd, dan wordt informatie over deze verbinding opgeslagen in een tabel (*state table*). Deze tabel staat meestal in het werkgeheugen van het systeem.

Netwerkpakketten die binnenkomen op het systeem worden vergeleken met de informatie die aanwezig is in deze tabel. Als het netwerkpakket herkend wordt als onderdeel van een al bestaande netwerkverbinding, dan wordt het zonder extra controles doorgelaten (dit wordt vaak in het Engels aangeduid als *cut through*).

Als in de tabel geen informatie over de bijbehorende verbinding van het netwerkpakket te vinden is (en het pakket dus geen onderdeel is van een al bestaande en gecontroleerde verbinding), dan wordt het pakket aan alle toegangsregels onderworpen (zoals bij het statische pakketfilter) en wordt het (afhankelijk daarvan) wél of niet toegelaten.

Het grootste voordeel van een dynamisch pakketfilter is dat de meeste pakketten niet met de lijst van filterregels vergeleken hoeven te worden, maar slechts met de lijst van bestaande verbindingen. Omdat deze test uitgevoerd wordt door een snelle zoekactie in het werkgeheugen van het systeem, wordt er een grote snelheidswinst behaald ten opzichte van het statische pakketfilter.

De informatie waarop het dynamische pakketfilter werkzaam is, is geschetst in figuur 3.4.



Figuur 3.4 Gebruikte informatie bij het dynamische pakketfilter

Er zijn twee gebieden waarop dynamische netwerkpakketfilters zich met name onderscheiden, te weten:
– het ondersteunen van multi-processorarchitecturen;
– de manier waarop initiële verbindingen totstandkomen.

Omdat het onderzoeken van elk netwerkpakket afzonderlijk plaatsvindt, kan dit in theorie goed parallel gedaan worden. Door systemen met parallelle processoren (SMP: Symetric Multi Processors) te gebruiken is de doorvoelsnelheid verbeterd.

Er zijn veel verschillende methoden om een tabel met gegevens over bestaande verbindingen te implementeren en te onderhouden. Bevindingen uit andere sectoren (als ontwikkeling van operating systemen, geheugenbeheer en hardwareontwikkeling) kunnen hier van dienst zijn. Implementatie en onderhoud van verbindingstabellen kunnen geoptimaliseerd worden op basis van de karakteristieken van het netwerkverkeer. Bij slechts enkele langdurige verbindingen zal een simpel lineair zoekalgoritme op de (kleine) tabel goed werken. Bij zeer veel kortdurende verbindingen zal een (grote) geïndexeerde hashtabel betere resultaten geven. Ook de levensduur van de informatie in de verbindingstabel en de wijze van schoning kunnen verbeterd worden. Dit zijn implementatiedetails die de verwerkingsnelheid kunnen beïnvloeden. De basale toepassing van de tabel blijft eender, namelijk antwoord geven op de vraag: 'Is dit pakket onderdeel van een al bestaande en geaccordeerde verbinding of niet?'

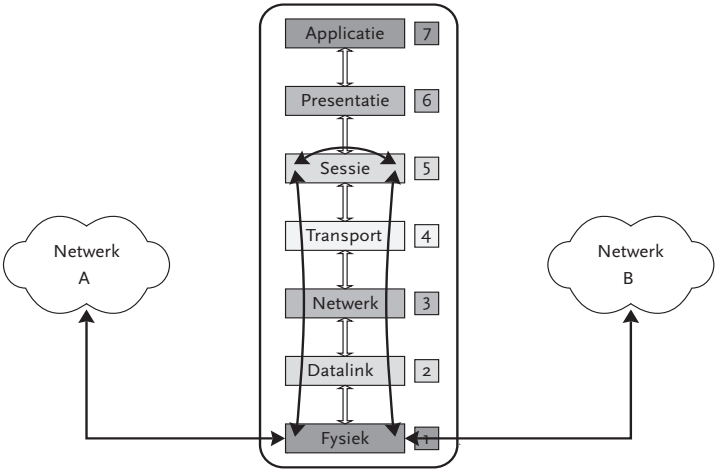
Er bestaat nog een andere methode om snelheidswinst te behalen, namelijk door af te wijken van de officiële standaarden en protocolstappen 'af te snijden'. De standaard voor het opzetten van een TCP/IP-verbinding is dat er een voorgeschreven dialoog plaats moet vinden tussen de zender en de ontvanger voordat een verbinding totstandkomt (de three-way handshake). Als deze standaard niet gevolgd wordt, en er direct bij het eerste pakket een verbinding wordt opgezet (en in de tabel wordt geplaatst), is er tijdwinst te boeken bij het opzetten van de verbinding. Deze methode is echter gevaarlijk omdat een hacker gebruik kan maken van een aanval met één pakket en een vervalst afzenderadres dat al in de verbindingstabel staat. Het filter neemt aan dat dit pakket bij een reeds bestaande verbinding hoort en zal het pakket accepteren.
De voor- en nadelen van het dynamische pakketfilter zijn samengevat in tabel 3.2.

Tabel 3.2 Overzicht dynamisch pakketfilter

Overwegingen voor een dynamisch netwerkpakketfilter	
Voordelen	***Nadelen***
Heeft de minste invloed op de verwerkingsnelheid van het systeem, vooral als er SMP-technieken goed worden toegepast	Werkt alleen op de netwerk- (en transport)-laag en onderzoekt daarom alleen de IP- en TCP-velden.
Lage aanschafkosten, veel besturingssystemen hebben deze functionaliteit tegenwoordig standaard	Niet bewust van de inhoud van het datapakketgedeelte, dit resulteert in een laag niveau van beveiliging
Door gebruik te maken van de status van verbindingen is er verbetering in doorvoersnelheid te bereiken	Kwetsbaar voor het veranderen van IP-adressen (IP spoofing)
	Moeilijk om regels in de juiste volgorde te definiëren
	Mogelijkheid om additionele risico's als verbindingen op te zetten zonder de RFC-standaard met de '3-way handshake' te gebruiken
	Verschaft een laag niveau van beveiliging

3.2.5 *Filter gebaseerd op netwerkverbindingen (circuit level gateway)*

Het circuit-level-gateway-filter werkt op de OSI-laag 5, de sessielaag. Naast de gebruikelijke controles die de andere pakketfilters op elk netwerkpakket uitvoeren, controleert dit type filter ook of de verbinding (in het Engels: *circuit*) volgens het juiste protocol tot stand wordt gebracht (via de three-way handshake) en of de volgorde van de netwerkpakketten binnen de verbinding klopt (via de *sequence numbers* van de netwerkpakketten). Figuur 3.5 toont het circuit-pakketfilter.

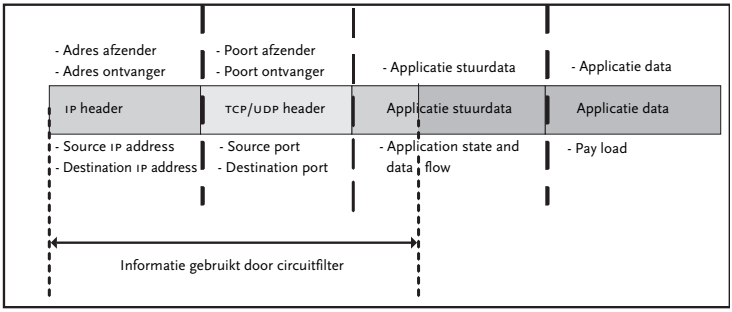


Figuur 3.5 Circuit-pakketfilter

Het beslissingsproces richt zich op de volgende velden van de IP- en TCP-headers:

- adres zender (source address);
- adres ontvanger (destination address);
- gebruikt protocol (application or protocol);
- verzendend programma (source port number);
- ontvangend programma (destination port number);
- opbouw van de verbinding (handshake);
- verloop van de verbinding (sequence numbers).

Dit type pakketfilter toetst dus meer informatie dan het statische en dynamische pakketfilter. Figuur 3.6 toont de gebruikte informatie bij het circuit-pakketfilter.



Figuur 3.6 Gebruikte informatie bij het circuit-pakketfilter

Net als de andere typen filters vergelijkt een circuit-pakketfilter de waarden in de IP- en TCP-velden met de waarden in de tabel met filterregels (de rule set). Daarnaast bekijkt het circuit-pakketfilter of de waarden van de SYN- en ACK-velden en de volgnummers passen bij de handshake tussen zender en ontvanger.

Als de waarden van de velden kloppen, wordt er in de tabel (de rule set) verder gezocht om de overige velden (de IP- en TCP-velden) te controleren. Dit zoeken gebeurt net zo lang tot er een expliciete overeenkomst met een filterregel gevonden is of tot de hele tabel is doorzocht zonder een expliciete overeenkomst te vinden. In dit laatste geval wordt de impliciete filterregel (*default rule*) toegepast die aangeeft dat 'alles wat niet is beschreven wordt doorgelaten' of 'alles wat niet is beschreven wordt geblokkeerd'.

Het circuit-pakketfilter biedt meer beveiliging dan de traditionele pakketfilters (die hiervoor beschreven zijn) en het kan zodanig geïmplementeerd worden dat de performance nauwelijks afneemt door de extra controles. Net als de overige filters heeft het echter een specifieke 'blinde vlek'. Na het totstandkomen van een legale verbinding wordt er verder geen controle meer uitgevoerd op de data binnen de netwerkpakketten.

Als eenmaal een verbinding tot stand is gebracht en als een mogelijkheid is gevonden om schadelijke data in de netwerkpakketten op te nemen, dan wordt dit niet opgemerkt door het filter.

Tabel 3.3 geeft een overzicht van het circuit-pakketfilter.

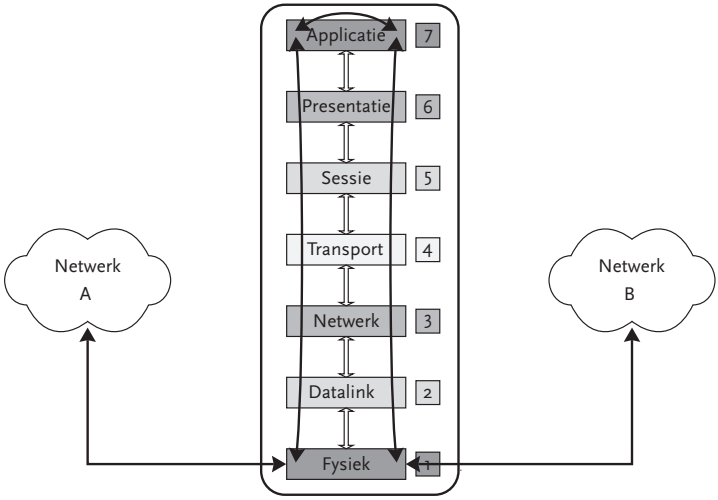
Tabel 3.3 Overzicht circuit-pakketfilter

Overwegingen voor een circuit-netwerkpakketfilter	
Voordelen	***Nadelen***
Lage tot middellage belasting voor de doorvoersnelheid	Veel van de nadelen van de pakketfilters zijn hier ook aanwezig
De verbinding naar een server verloopt in twee stappen door het filter waardoor er meer controle is	Er wordt niet gecontroleerd op inhoud van de verbinding
Hoger niveau van beveiliging dan een statisch of dynamisch pakketfilter	Verschaft een laag tot middellaag niveau van beveiliging

3.2.6 Filter gebaseerd op de toegepaste applicatie (application level gateway/proxy)

Net als het circuit-pakketfilter zal het applicatie-pakketfilter de binnenkomende en uitgaande netwerkpakketten onderscheppen, controleren en de inhoud expliciet doorgeven indien dit is toegestaan door de rule set.

Dit type filter wordt meestal aangeduid met de Engelse term *proxy server* (*proxy* betekent 'stroman' of 'tussenpersoon'). Door een proxyserver wordt de directe verbinding tussen twee communicerende systemen doorbroken en gesplitst in twee helften. Eén helft loopt van de zender naar de proxy en de andere helft loopt van de proxy naar de ontvanger (en vice versa). Figuur 3.7 toont het applicatie-pakketfilter.

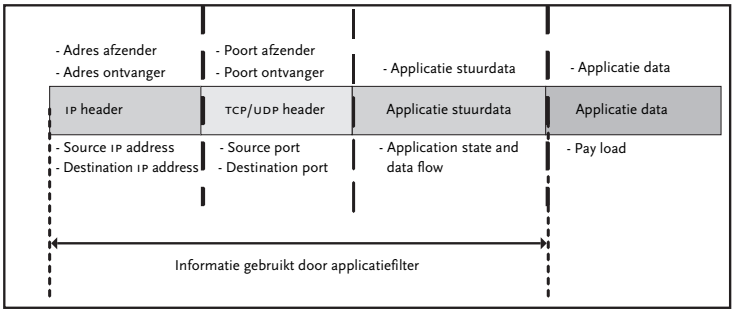


Figuur 3.7 Applicatie-pakketfilter

Het beslissingsproces richt zich op de volgende informatie uit de IP- en TCP-headers en datavelden:

- adres zender (source address);
- adres ontvanger (destination address);
- gebruikt protocol (application or protocol);
- verzendend programma (source port number);
- ontvangend programma (destination port number);
- opbouw van de verbinding (handshake);
- verloop van de verbinding (sequence numbers);
- applicatiespecifieke informatie uit de datavelden, met name de commando's die aan de applicatie worden gegeven en de functies die worden aangeroepen.

Figuur 3.8 toont de gebruikte informatie bij het applicatie-pakketfilter. Dit type pakketfilter controleert op meer informatie dan het statische en dynamische pakketfilter. Het applicatie-pakketfilter controleert naast de opbouw en de volgorde van de verbinding, zoals het circuit-pakketfilter deed, ook de specifieke applicatie-opdrachten die tijdens de communicatie gegeven worden.



Figuur 3.8 Gebruikte informatie bij het applicatie-pakketfilter

Drie belangrijke verschillen tussen het circuit-netwerkfilter en de proxy (het applicatie-pakketfilter) zijn dat de proxy's:
– op de OSI-applicatielaag kunnen werken;
– het gehele netwerkpakket controleren (headers en datavelden);
– applicatiespecifiek zijn.

In tegenstelling tot de voorgaande filters accepteert en verwerkt een proxy alleen netwerkpakketten van programma's en services die de proxy (her)kent en waarvan de proxy weet wat de inhoud van de netwerkpakketten betekent. Dit wil echter ook zeggen dat een proxy alleen die protocollen kan verwerken die de proxy begrijpt (protocollen waarvoor er kennis is ingebouwd in de filterprogrammatuur). Als er bijvoorbeeld proxyfunctionaliteit aanwezig is voor de FTP- en HTTP-protocollen, dan zullen alleen deze twee services doorgelaten kunnen worden. Alle andere services zullen door de proxy niet gecontroleerd en dus geweigerd worden.

Het applicatie-pakketfilter bekijkt elk individueel netwerkpakket. Ook worden de datavelden in de netwerkpakketten gecontroleerd en wordt nagekeken of deze gegevens toegestane of verboden opdrachten bevatten. Binnen het FTP-programma kan bijvoorbeeld op het commando PUT gefilterd worden en hiermee wordt ongeautoriseerde wijziging van gegevens verhinderd.

Door de proxy wordt de inhoud van elk inkomend netwerkpakket expliciet gecontroleerd, en mogelijk verdachte gegevens worden uit het net-

werkpakket verwijderd. Vervolgens geeft de proxy een 'schoon en veilig' netwerkpakket door aan de ontvanger. Hierdoor wordt manipulatie van netwerkpakketten verhinderd en wordt een hele klasse van misbruik (*covert channels*) tegengegaan.

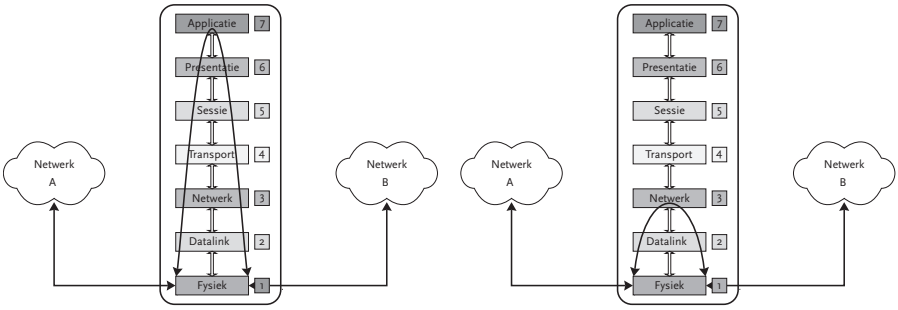
Door de expliciete controle en schoning van netwerkpakketten is de proxy het krachtigste filter van de tot nu toe besproken typen filters. Moderne applicatie-pakketfilters zijn dermate transparant voor de eindgebruikers dat het niet opvalt dat hun verbindingen via een proxy lopen. Tabel 3.4 geeft een overzicht van het applicatie-pakketfilter.

Tabel 3.4 Overzicht applicatie-pakketfilter

Overwegingen voor een applicatie-netwerkpakketfilter	
Voordelen	***Nadelen***
Applicatie-netwerkpakketfilters die op SMP-machines geïmplementeerd worden, laten slechts een lichte impact zien op de performance	Een slechte implementatie van een proxy kan zeer veel impact hebben op de netwerkperformance
Doordat de verbinding in twee stukken wordt gehakt en er een expliciete kopieerslag van alleen dat wat is goedgekeurd plaatsvindt, vervalt de hele klasse van covert channels-aanvallen	Het is niet triviaal om een veilige proxy te schrijven en niet een die zelf een aantal beveiligingszwakheden heeft, zoals buffer overrun
Proxy's die ook de protocol-headerlengte controleren, kunnen een aantal buffer overrun-aanvallen tegengaan	De proxy-software moet voortdurend aangepast worden aan de nieuwste protocollen en functies
Hoogste beveiligingsniveau	Een slechte proxy-implementatie en afhankelijkheden van het besturingssysteem kunnen ervoor zorgen dat er simultaan te weinig verbindingen mogelijk zijn

3.2.7 *Filter gebaseerd op combinaties van meerdere technieken (hybrid inspection)*

De verschillende typen netwerkfilters die hierboven beschreven zijn, kunnen worden gecombineerd. Het hybride pakketfilter is een van de resultaten van een dergelijk combinatie. Dit filter heeft de mogelijkheid om op alle zeven lagen van het OSI-model controles uit te voeren en de specifieke context bij te houden. Dit is weergegeven in het linkergedeelte van figuur 3.9.



Figuur 3.9 Hybride pakketfilter

In de praktijk blijkt echter dat dit soort filters niet met alle OSI-lagen werkt, maar alleen contextgevoelige informatie gebruikt op de netwerklaag, gebaseerd op het IP-adres van de zender, het IP-adres van de ontvanger en de poortnummers. Deze beperkte blik van het filter wordt nog versterkt door het feit dat het contextgevoelig filteren op hogere lagen zo veel performance vraagt dat firewall-beheerders de functie meestal uitzetten. Hierdoor ontstaat schijnbeveiliging. Dit is weergegeven in het rechtergedeelte van figuur 3.9.

Zoals eerder aangegeven kan het circuit-pakketfilter contextgevoelige controles uitvoeren om te bepalen of de volgorde en het type van netwerkpakketten logisch consistent zijn. Deze functionaliteit wordt echter vaak geïmplementeerd op het dynamische pakketfilterniveau, waarbij de contextinformatie verloren gaat en niet voor de controle gebruikt kan worden. Dan is het mogelijk om met een enkel netwerkpakket een net-

werkverbinding op te zetten door het SYN-bit aan te zetten. Verder is het zo dat bij sommige implementaties de controle alleen correct wordt uitgevoerd op netwerkverkeer dat van buiten naar binnen loopt. Dit opent de mogelijkheid om vanuit het bedrijfsnetwerk (vanuit 'binnen') verbindingen op te zetten die verder niet gecontroleerd worden.

Net als bij een applicatie-pakketfilter, kan een hybride pakketfilter zo geconfigureerd worden dat het netwerkpakketten met een riskante inhoud niet doorgeeft. Een FTP-netwerkpakket dat een PUT-commando bevat kan geblokkeerd worden. De performance gaat door deze controles echter zo veel achteruit dat firewall-beheerders deze functionaliteit vaak uitzetten en terugvallen op het niveau van dynamische pakketfiltering.

Tabel 3.5 Overzicht hybride pakketfilter

overwegingen voor een *hybrid inspection*-netwerkpakketfilter	
Voordelen	***Nadelen***
Biedt de mogelijkheid om op al de OSI-lagen te controleren en kan door de beheerder geconfigureerd worden	De benodigde performance van een niet-SMP-machine is dermate hoog dat veel beheerders ervoor kiezen dan een dergelijk filter in te zetten op het dynamisch netwerkpakketfilterniveau
De netwerkstroom tussen zender en ontvanger wordt niet in twee stukken gebroken	Het niet in tweeën hakken van de netwerkverbinding zien sommigen als een onacceptabel beveiligingsrisico, aangezien er direct contact mogelijk is tussen de zender en de ontvanger
Het is mogelijk om een geïntegreerd, dynamisch en *stateful* netwerkpakketfilter te creëren	Een slechte proxy-implementatie en afhankelijkheden van het besturingssysteem kunnen ervoor zorgen dat er simultaan te weinig verbindingen mogelijk zijn
Snelle performance toegepast als een dynamisch netwerkpakketfilter. Echter door gebruik van SMP-technieken zijn vele echte dynamisch netwerkpakketfilters sneller	Er zijn op dit moment nog geen hybrid inspection-netwerkpakketfilters bekend die een voldoende hoge beveiligingcertificering hebben (bijvoorbeeld hoger dan de EAL 2 niveau van de *common criteria*)

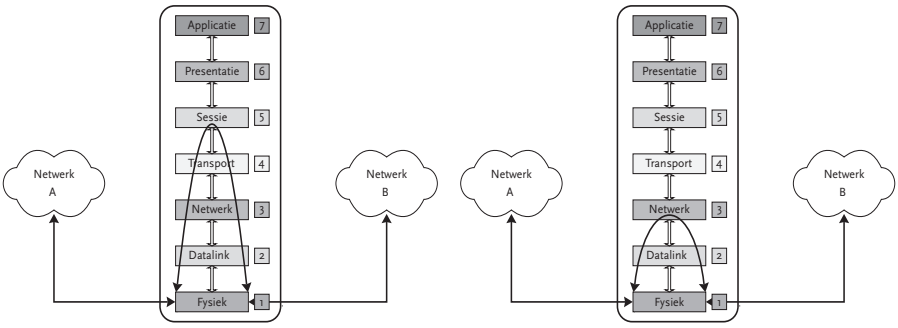
In tegenstelling tot een applicatie-pakketfilter, breekt een hybrid-inspection-filter de verbinding niet in twee stukken en wordt de inhoud van netwerkpakketten niet geschoond en (her-)verpakt in een betrouwbaar netwerkpakket. Wel is het mogelijk om op alle OSI-lagen te controleren, dus ook op de commando's van specifieke programma's. Dit kost echter veel performance, waardoor hybrid inspection meestal niet wordt toegepast op alle lagen van het OSI-model, maar vaak alleen op de lagen 1 tot 4. Tabel 3.5 geeft een overzicht van het hybride pakketfilter.

3.2.8 Filter gebaseerd op snelheid (cutoff proxy)

De cutoff proxy is een combinatie van een dynamisch pakketfilter en een circuit-pakketfilter, al dan niet contextgevoelig (*stateful*).

Bij elke nieuwe netwerkverbinding gedraagt het filter zich als een circuit-pakketfilter door te controleren op het juist uitvoeren van de opbouw van een TCP-verbinding (three-way handshake). Als die succesvol is verlopen, schakelt het filter om naar een dynamisch pakketfilter. Hierdoor wordt performancewinst geboekt omdat een dynamisch pakketfilter op een lagere OSI-laag werkt en zijn controles sneller kan uitvoeren.

Figuur 3.10 toont het cutoff-proxy-pakketfilter.



Figuur 3.10 Cutoff-proxy-pakketfilter

Het is goed om op te merken dat de cutoff proxy niet een echte *application level proxy* is; de netwerkverbinding wordt niet in tweeën gebroken. Dit biedt minder bescherming, maar de performance is beter. Tabel 3.6 geeft een overzicht van het cutoff-proxy-pakketfilter.

Tabel 3.6 Overzicht cutoff-proxy-pakketfilter

Overwegingen voor een cutoff proxy-netwerkpakketfilter	
Voordelen	***Nadelen***
Minder performance nodig dan een 'echte' circuit level proxy	Het is en blijft geen circuit-netwerk-pakketfilter, maar iets wat er op lijkt
Het veranderen en misbruiken van verkeerde adresgegevens is geminimaliseerd omdat de tcp opbouw expliciet gecontroleerd wordt.	Door het niet in tweeën breken van de netwerkverbinding zijn veel van de problemen die een dynamisch netwerk-pakketfilter kent ook hier aanwezig.
	Niet in staat om de inhoud van de data te interpreteren
	Kan een schijnveiligheid creëren door gebrek aan besef dat het niet een circuit-netwerkpakketfilter is

3.2.9 Filter dat netwerken 'gescheiden' houdt (air gap)

Sinds enige tijd is er een ander type filter geïntroduceerd. Dit type wordt aangeduid als het air-gapfilter, omdat er eigenlijk geen sprake is van het doorlaten van netwerkverkeer. De onderliggende techniek gaat ervan uit dat er geen verbinding wordt opgezet tussen zender en ontvanger, maar eerst tussen zender en filter en daarna tussen filter en ontvanger.

De uit te wisselen gegevens worden door het filter ontvangen en opgeslagen op een harde schijf of in het werkgeheugen. Hierna wordt de verbinding met de zender verbroken. Na controle van de gegevens wordt de verbinding met de ontvanger geactiveerd en worden de gegevens door het filter aan de ontvanger doorgegeven. De werking lijkt enigszins op de werking van het applicatie-pakketfilter.

De afname in performance (vooral indien er een harde schijf gebruikt wordt) is dermate groot dat deze optie onbruikbaar is voor die situaties waarin meerdere verbindingen tegelijk nodig zijn. De meningen over het nut en noodzaak van deze technologie zijn nog verdeeld. Tabel 3.7 geeft een overzicht van het air-gapfilter.

Tabel 3.7 Overzicht air-gapfilter

Overwegingen voor een air gap-netwerkpakketfilter	
Voordelen	***Nadelen***
De verbinding tussen zender en ontvanger wordt daadwerkelijk in tweeën gebroken zodat bijvoorbeeld covert channels-aanvallen niet mogelijk zijn	Grote negatieve invloed op de performance
Het gebruikmaken van een sterke applicatieproxy kan buffer overrun-aanvallen voorkomen	Net zoals bij applicatie-netwerkpakketfilters moeten de leveranciers bijblijven en de nieuwe programmatuur en functionaliteit ondersteunen
Net zoals applicatie-netwerkpakketfilters kan een air gap-filter een hoog niveau van beveiliging realiseren	Er is geen enkele externe certificering bekend voor deze apparatuur

3.3 Positioneren van filters

Het is duidelijk dat er niet één ideaal filter bestaat dat in alle omstandigheden geschikt is. Aanschafkosten, performance, mate van complexiteit en mate van benodigde ondersteuning zijn criteria die van invloed zijn op de uiteindelijke keuze van het type filter of firewall. De afweging van alternatieven, gerelateerd aan het belang voor de organisatie, wordt behandeld in hoofdstuk 4.

Op dit moment dalen de kosten van firewalls steeds meer (ze zijn tegenwoordig gecombineerd met routers voor een redelijke prijs te koop), terwijl de performance en functionaliteit van firewalls alleen maar toenemen. Dit maakt de afweging van alternatieven eenvoudiger. Het gebruik

van een firewall hoeft niet beperkt te blijven tot het koppelpunt tussen internet en bedrijfsnetwerk. Firewalls kunnen ook binnen bedrijfsnetwerken toegepast worden, bijvoorbeeld in de vorm van centraal beheerde, maar fysiek gedistribueerde firewalls. Dit zou er uiteindelijk toe kunnen leiden dat elk computersysteem dat communiceert met andere systemen zelf een ingebouwde firewall heeft (wat bijvoorbeeld al het geval is met vele thuiscomputers die voorzien zijn van een *personal* firewall).

4 Functionaliteiten van een firewall

4.1 Inleiding

De functionaliteit van een moderne firewall bestaat uit verschillende bouwblokken. Deze bouwblokken richten zich op een aantal basisfuncties die hieronder beschreven worden. Een aantal functies is generiek voor alle firewalls. Zo is het eerste bouwblok 'pakketfiltering' zo basaal dat alle firewalls deze functionaliteit hebben, ongeacht merk en type. Je zou zelfs kunnen zeggen dat ze zonder deze functionaliteit geen firewalls zijn! De meeste, zo niet alle, firewalls hebben tegenwoordig ook de functie NAT/PAT (*network address translation/port address translation*) in hun basispakket. Waar de set van basisfuncties ophoudt en de set van *add-ons* (extra toegevoegde functies) begint, is arbitrair en levert vaak discussies op. In deze studie wordt in het midden gelaten welke functies precies als basisfuncties in aanmerking komen.

Een oud en vertrouwd onderwerp is de richting waarin gefilterd moet worden. Bij een firewall met drie netwerkinterfaces zijn er bijvoorbeeld zes verschillende netwerkstromen waarop beslissingen genomen kunnen worden. Hierop zijn variaties mogelijk die het aantal combinaties verder doet toenemen, zoals al het uitgaande verkeer op een bepaalde interface (dus onafhankelijk waar het vandaan komt). Hierbij is het altijd belangrijk te bepalen wat er bedoeld wordt met termen als 'binnen'/'buiten', 'in'/'uit', enzovoorts. Er wordt discussie gevoerd over de beveiligingsniveaus van de domeinen waartussen filtering plaatsvindt. Zo zal het buitennetwerk vaak een lager beveiligingsniveau hebben dan het binnennetwerk.

Het jarenlange gebruik van firewalls heeft ons voornamelijk één inzicht opgeleverd, namelijk dat een firewall niet feilloos is. Keer op keer wordt de beveiliging van een firewall doorbroken; door een nieuwe technologie waarvoor nog geen of onvoldoende regels zijn, of door nieuw en soms oneigenlijk gebruik van oudere protocollen op een manier die niemand voorzien had. Dit doorbreken van de beveiliging wordt in het Engels aangeduid als *intrusion* en de discussie gaat in deze context vooral over de concepten van *intrusion detection* en *intrusion prevention*. Het is het doel van een firewall om dat wat niet is toegestaan, tegen te houden en hierdoor te voorkomen dat ongewenste dingen plaatsvinden op het netwerk. In die zin worden incidenten voorkomen en kan de firewall worden gezien als een realisatie van het concept van intrusion prevention.

Een relatief nieuw fenomeen waar firewalls mee van doen krijgen, is het garanderen van doorvoersnelheid in applicaties die tijdskritisch zijn. Dit wordt aangeduid met de Engelse term *Quality of Service* (QoS). Een voorbeeld is het H.323-protocol dat gebruikt wordt om *Voice-over-IP* (VoIP) te realiseren. Dit protocol is erg tijdsgevoelig; als de verwerking van de netwerkstroom te lang duurt of te onregelmatig is, dan treedt er merkbaar kwaliteitsverlies op, iets wat als hinderlijk wordt ervaren (bij het bellen via internet). Naast VoIP zijn er diverse andere protocollen die deze eigenschap hebben.

Een ander aspect dat te maken heeft met het garanderen van de verwerkingssnelheid van firewalls, is de aanval van *[Distributed] Denial of Service* ([D]DoS), waarbij het slachtoffer zo veel (onzinnig) werk te doen krijgt dat er weinig effectief (zinnig) werk meer gedaan kan worden. Als de firewall de snelheid en de hoeveelheid van het inkomend verkeer met een bepaald afzenderadres zou beheersen, dan kan voorkomen worden dat de firewall te veel tijd besteedt aan één netwerkstroom. Dit concept heet *rate limiting* en wordt bij de grotere firewalls vaak al standaard toegepast.

Hoewel de basis van elke vorm van netwerkbeveiliging uitgaat van het filteren van netwerkpakketten of -connecties, wordt dit op zichzelf staand niet meer beschouwd als een adequate beschermingsmaatregel. De huidige typen firewalls die gebruikt worden binnen bedrijven, combineren meer functionaliteiten dan alleen het op basis van toegangslijsten verbieden of toestaan van netwerkpakketten.

De huidige firewalls combineren diverse technieken om controle over zowel de connectie als de data die via de connectie verstuurd wordt, te *screenen*. In dit hoofdstuk zullen verschillende onderdelen van deze firewalls besproken worden. Of deze onderdelen geïntegreerd in één platform of als separate functionaliteit moeten worden opgenomen, is van vele factoren afhankelijk, en de keuze zal in de regel tijdens het uitwerken van de ontwerpcriteria gemaakt worden. De functies worden in deze studie als onderdeel van een firewall-omgeving gezien en behandeld.

4.2 Pakketinspectie

De basis van elke netwerkbeveiliging is pakketfiltering. Hiertoe zijn regels opgesteld die op de onderste lagen van de ISO-OSI-protocolstack ingrijpen. Er zijn verschillende vormen van pakketfiltering. Deze worden in dit hoofdstuk besproken.

Alle vormen van IP-filtering gaan uit van IP-adressen. Een IP-adres bestaat altijd uit 32 bits, die vaak worden weergegeven in vier decimale getallen gescheiden door punten (bijvoorbeeld 192.43.15.211). Een IP-adres heeft twee logische delen, een netwerkadres en een hostadres. Daarnaast wordt er een masker meegegeven. Het masker en het IP-adres geven samen informatie over het IP-netwerk waar een host onderdeel van is.

IP-adressen van zowel hosts als netwerken bestaan uit vier octetten (groepen van 8 bits die worden weergegeven in decimale getallen met een waarde tussen 0 en 255) en kunnen op twee manieren worden genoteerd. De internationale schrijfwijze voor IP-adressen is vier octetten voor het host- of netwerkadres, gevolgd door vier octetten voor het masker, 10.0.0.1 255.255.255.0, of vier octetten voor het adres met alleen het aantal bits van het masker, 10.0.0.1/24.

IP-adressen worden op internet beheerd en uitgegeven door zogenaamde Network Coördinator Centres. In Europa is dit RIPE. Een aantal netwerkadressen wordt niet uitgegeven. Deze adressen zijn beschreven in RFC 1918 en zijn alleen bedoeld voor intern gebruik.

Elke connectie tussen twee netwerkstations zal een afzender-IP-adres en een bestemming- IP-adres hebben. Belangrijke velden voor pakketfiltering zijn, naast de IP-adressen, de TCP-poortnummers (afzender en bestemming), bij het gebruik van dynamische pakketfiltering de additionele TCP-velden zoals SYN, ACK, RST en FIN en de sequence-nummers (zie ook hoofdstuk 3 over het IP- en TCP-protocol).

4.2.1 Statische pakketfiltering

De simpelste verschijningsvorm van een firewall is het statische pakketfilter. Een voorbeeld van een dergelijk filter is de *Acces Control List* (ACL). In de routers van bekende fabrikanten is deze functionaliteit in de vorm van ACL's aanwezig. Ook in besturingssystemen die geschikt zijn om te routeren, komt deze filtering voor.

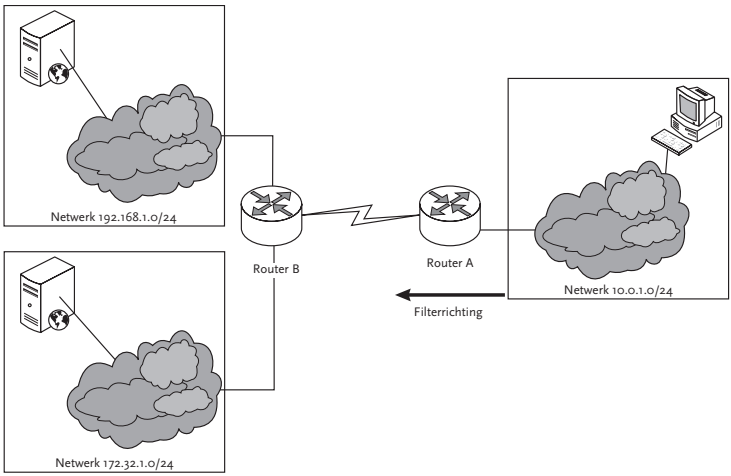
Bij statische pakketfiltering wordt op basis van IP-adressen een lijst gemaakt waarop wordt aangegeven of een pakket verwerkt moet worden in de router of niet. Doordat deze filtermethode geen rekening hoeft te houden met connecties en elk pakket separaat bekijkt, kost deze methode de minste rekenkracht, maar geeft die ook de minste beveiliging.

In de praktijk wordt statische pakketfiltering voornamelijk gebruikt op locaties in het netwerk waar op hoofdlijnen moet worden gefilterd, zonder dat dit een grote invloed mag hebben op de doorvoersnelheid. Een voorbeeld van statische pakketfiltering is het filteren van netwerkverkeer gegenereerd door virussen op zo veel mogelijk koppelpunten tussen netwerken.

Een voorbeeld van een Cisco-ACL is het verbieden van netwerkverkeer vanuit netwerk 10.0.1.0 naar netwerk 192.168.1.0, maar het toestaan van netwerkverkeer vanuit netwerk 10.0.1.0 naar netwerk 172.32.1.0. Zie figuur 4.1 en figuur 4.2.

```
access-list 100 deny ip    10.0.1.0 0.0.0.255  192.168.1.0 0.0.0.255
access-list 100 permit ip 10.0.1.0 0.0.0.255  172.32.1.0 0.0.0.255
```

Figuur 4.1 Voorbeeld 1 ACL-commando's



Figuur 4.2 Voorbeeld 1 ACL grafisch

4.2.2 Stateful inspection

De meeste firewalls ondersteunen *stateful inspection*. Deze vorm van filteren geeft een betere beveiliging dan statische pakketfiltering, omdat de firewall nu ook informatie over sessies en het protocol bijhoudt en daarmee een gefundeerde beslissing kan nemen over verkeersstromen.

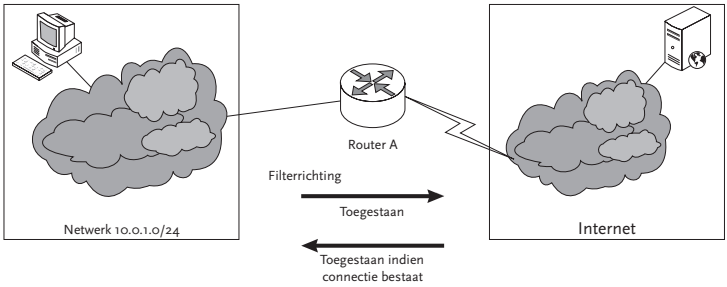
Door de three-way handshake, die plaatsvindt op TCP-niveau, kan de firewall een tabel opbouwen. Aan de hand van de handshake en in combinatie met de volgnummers, wordt bijgehouden welke inkomende datastroom bij welke uitgaande data-aanvraag hoort. Dit geeft een betere controle op inkomend verkeer dan bij statische pakketfiltering, maar is zoals ook beschreven in paragraaf 3.2.3 geen garantie dat er geen ongewenst verkeer gebruik kan maken van zwakheden in het TCP/IP-protocol.

Hoe kan stateful inspection in bijvoorbeeld een Cisco-router geconfigureerd worden? Een Cisco-router is gekoppeld aan het internet. De pc's op het netwerk 10.0.1.0/24 mogen verbinding maken met internet. Vanaf internet mag géén connectie worden gemaakt met systemen op dit net-

werk. In Cisco-routers zorgt het sleutelwoord *establised* voor de stateful inspection, door verkeer alléén naar binnen door te laten als er een overeenstemmende connectie is opgezet naar buiten toe. Het sleutelwoord kijkt in het *flags*-veld van de TCP-header naar de vlaggen RST of ACK. Alléén pakketten met een van deze vlaggen aan worden toegelaten, overige pakketten dus niet. Dit mechanisme is niet bestand tegen zogenaamde *crafted packets*, waarin met behulp van malafide software pakketten worden gefabriceerd met de RST- of ACK-vlag aan. In dit voorbeeld wordt er dus alléén netwerkverkeer toegestaan naar netwerk 10.0.1.0/24 als er een aanvraag vanuit het netwerk 10.0.1.0/24 is gekomen. Zie figuur 4.3 en figuur 4.4.

```
access-list 100 permit ip any  10.0.1.0 0.0.0.255 established
access-list 100 deny ip any    10.0.1.0 0.0.0.255
```

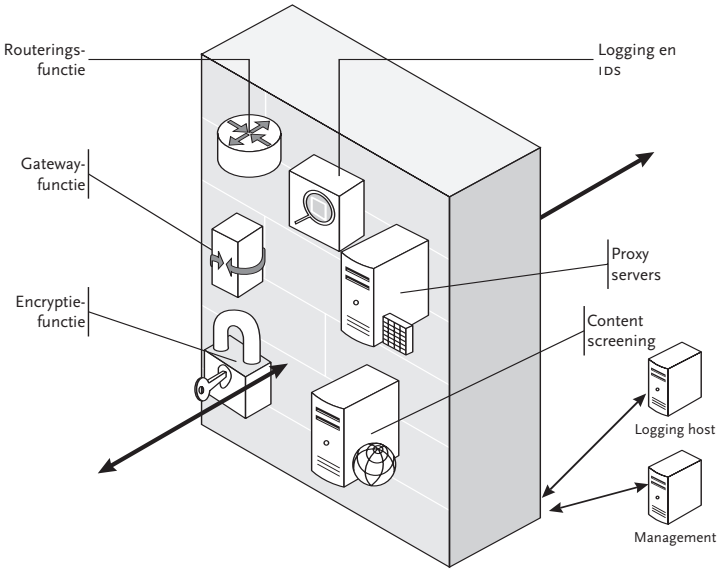
Figuur 4.3 Voorbeeld 2 ACL-commando's



Figuur 4.4 Voorbeeld 2 ACL grafisch

4.2.3 Hybride inspectie

Hybride inspectie is een combinatie van alle hierboven genoemde filtermethodes in combinatie met de verschillende add-ons zoals hierna besproken. De op de markt verkrijgbare *Enterprise Class Firewalls* (Cisco PIX, CheckPoint Firewall 1, Juniper Netsceen) werken alle in meer of mindere mate met een toepassing van hybride inspectie. Zie ook figuur 4.5.



Figuur 4.5 Hybride firewall

Door de verschillende filtertechnieken te combineren met de verschillende proxytechnieken kunnen de specifieke tekortkomingen van de losse technieken worden vermeden. Een van de nadelen van hybride inspectie, vergeleken met de in de vorige paragraaf genoemde filtermethodes, is de complexiteit van de configuratie.

4.3 Applicatie-inspectie (proxyservers)

Er bestaan in hoofdlijnen twee verschillende soorten proxyservers: *Application Level Firewalls* en *Connection Level Firewalls*.

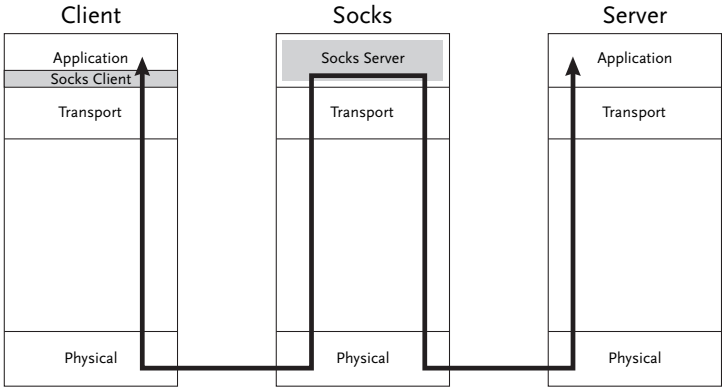
Als netwerkoplossing wordt meestal gekozen voor een zogenaamde *dual homed* proxyserver. Een dual homed proxyserver heeft twee netwerkinterfaces, één in het interne netwerk met een intern adres en één netwerkinterface met een op internet routeerbaar (extern) adres. Als interne systemen een sessie willen opzetten met internet, zullen deze sessies feitelijk worden opgezet door middel van de proxyserver, die op zijn

beurt een sessie opzet met het internetsysteem. Door het internetadres van de proxyserver te gebruiken worden de interne adressen als het ware naar een internetadres vertaald. Proxyservers zorgen ervoor dat er geen directe IP-connectie tussen aanvrager en *resource* bestaat. De connecties zijn er tussen aanvrager en proxy, en tussen proxy en resource.

Omdat een proxyserver connecties op IP-basis termineert en sessies doorlaat, kunnen we spreken van Application Level Firewalls en Connection Level Firewalls.

4.3.1 Connection Level Firewalls

Het bekendste en meest verspreide voorbeeld van een Connection Level Firewall is het Socks-protocol (of de Socks-applicatie). De Socks-proxy bestaat uit een client/server-toepassing. De Socks-client op een hostsysteem zal connectie maken met de Socks-server. Via deze connectie kunnen applicaties op het hostsysteem de Socks-server verzoeken om met resources op een ander *device* connecties te maken. De proxy heeft geen weet van het protocol, maar fungeert als TCP-connectieproxy. De TCP-connectie wordt tussen aanvrager en proxy en tussen proxy en resource opgezet.



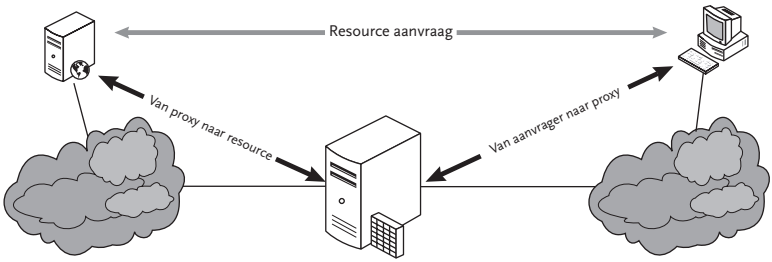
Figuur 4.6 Connection Level Firewall

Doordat de Socks-proxy niet applicatie-afhankelijk is, zoals de Application Level Firewalls, kunnen alle applicaties die gebruikmaken van een computer waar een Socks-client op geconfigureerd is, met behulp van deze proxy connecties maken. In figuur 4.6 is een Connection Level Firewall afgebeeld.

4.3.2 Application Level Firewalls

Het grote verschil tussen een Application Level Firewall (in de volksmond: proxy) en een pakketfilter is dat een Application Level Firewall contact opneemt met de gevraagde resources in plaats van met de client, terwijl een pakketfilter op basis van filterregels connecties in zijn geheel toelaat of verbiedt.

Om contact op te nemen met gevraagde resources moet het connectieverloop van een IP-sessie bekeken worden. Om een resource op een netwerk op te vragen maakt het vragende station een IP-connectie tussen zichzelf en het station waar de resource zich bevindt. Een pakketfilter onderbreekt deze connectie niet. Een Application Level Firewall daarentegen zal als tussenstation fungeren: het vragende station zet een connectie op met een Application Level Firewall, de Application Level Firewall neemt contact op met het station waar de resource zich bevindt en zal afhankelijk van het soort proxy de resource eerst zelf verwerken, alvorens deze naar het vragende station door te sturen. Figuur 4.7 brengt de Application Level Firewall in beeld.



Figuur 4.7 Application Level Firewall

Door de onderbreking kan een Application Level Firewall de opgevraagde resources (*content*) beter beoordelen en, in het geval van een zogenaamde *caching proxy*, deze ook gedurende enige tijd bewaren. Hierdoor zullen vervolgaanvragen voor dezelfde content niet meer vanaf het originele station opgehaald worden, maar direct uit de lokale opslagplaats worden verstuurd. Nadeel is dat voor elke connectie een separaat proces gestart moet worden op de server, en voor elke soort connectie (of protocol) een separate Application Level Firewall worden ingericht. Dus voor tweehonderd connecties naar webservers moeten er tweehonderd processen gestart worden.

Enkele bekende voorbeelden van Application Level Firewalls zijn Squid, een *open source*-HTTP-proxy, en SAP-router, een applicatieproxy voor SAP.

4.3.3 Contentscreening en -filtering

Als een firewall beschouwd wordt als het hek om het vliegveld, dan zijn contentscreening en -filtering de douaniers die de koffers op het vliegveld openen en inspecteren. Er is in eerdere hoofdstukken al aandacht besteed aan de controle van netwerkconnecties, maar steeds vanuit het oogpunt van TCP/IP. Er werd voorbij gegaan aan de informatie die verstuurd en/of ontvangen kan worden via een netwerkconnectie, terwijl er wel degelijk een ongewilde informatiestroom kan zijn.

Adresfiltering

De eenvoudigste vorm van contentscreening of -filtering is op basis van een zogenaamde *black list* of *white list*. Een black list geeft aan wat niet mag, de rest mag wel. Een white list is het tegenovergestelde, deze geeft aan wat wel mag, de rest mag dus niet. Met het gebruik van deze lijsten wordt niet alleen gefilterd op basis van IP-informatie, maar wordt op basis van de lijst ook bekeken of de aanvraag het netwerk mag verlaten.

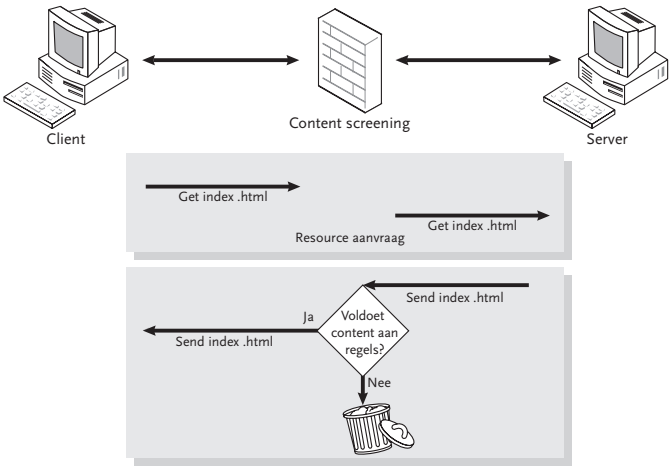
Bij een implementatie van contentfiltering op basis van dit soort lijsten wordt door een leverancier, of de eigen organisatie, een lijst met netwerkadressen samengesteld (URL's of IP-adressen) waarvandaan content expliciet wel of expliciet niet (afhankelijk van een black of white list) mag worden bekeken (*implicit permit, deny on list*).

Nadeel van het black list-systeem is dat de lijst op basis van URL's werkt, die bijgehouden moeten worden. Gezien de snelle wijzigingen op internet zal de black list altijd achterlopen op de werkelijke situatie. Het bijhouden van een black list betekent dat er menselijk handelen noodzakelijk is om alle sites die volgens de geldende policy niet bekeken mogen worden, toe te voegen. Men kan er ook voor kiezen het aantal sites dat bezocht mag worden te beperken door middel van een white list (*implicit deny, permit on list*).

Deze laatste mogelijkheid beperkt echter zeer sterk het gebruik van internet als globale kennisbank, en hoeft niet te betekenen dat ongewilde sites niet bezocht worden. Door gebruik te maken van een zogeheten *remoteproxy* is het toch mogelijk ongewenste sites te bekijken. Een goed voorbeeld van een remoteproxy is de *caching*-functie van Google. Er wordt dan niet rechtstreeks gekeken naar de verboden server met ongewenste content maar naar een proxyserver.

Datafiltering

Door de verbeterde techniek is het niet alleen mogelijk om op basis van TCP/IP informatie te filteren op een firewall, maar deze filtering ook uit te breiden naar de inhoud van de pakketten, de zogenaamde *payload*.



Figuur 4.8 Datafiltering

Verschillende firewall-implementaties kennen deze functionaliteit. Contentfiltering vergt echter aanzienlijke verwerkingscapaciteit. Om die reden wordt er vaak voor gekozen om contentfiltering niet door de firewall zelf te laten uitvoeren, maar door een proxyserver. Zie figuur 4.8.

Een grote uitdaging voor een firewall is het bijhouden van alle netwerkconnecties, en eventueel het samenvoegen van de afzonderlijke pakketten zodat de inhoud (payload) ook daadwerkelijk zichtbaar wordt.

Een voorbeeld: een simpele HTTP-vraag om de indexpagina van www.yahoo.com op te vragen bestaat uit meerdere IP-pakketten, eerst een aantal om de sessie te initiëren, dan een HTTP-Get-opdracht. Als resultaat van deze HTTP Get en de daaropvolgende Gets wordt de inhoud van een pagina verstuurd naar de browser. Om te kunnen bepalen of de inhoud voldoet aan de opgestelde regels, moet een firewall dus de complete sessie samenstellen.

Omdat dit een behoorlijke belasting betekent, zal er in grotere omgevingen voor gekozen worden om dit proces op een proxy uit te voeren en op de firewall slechts URL's te filteren. In een URL kan overigens ook al informatie verborgen liggen waarover een besluit kan worden genomen, denk hierbij bijvoorbeeld aan een HTTP-Get-opdracht voor een file met de extensie '.mp3'.

Actieve webcomponenten als Active-X en Java dragen een risico in zich. Deze componenten worden uitgevoerd in de programmatuur van de opvragende computer en kunnen zich dus gedragen als niet-geautoriseerde programma's, met alle risico's van dien. In een goedbeveiligde omgeving is het dan ook noodzakelijk om ook op deze content te screenen. Op basis van een rule set kan worden bepaald of deze actieve componenten mogen worden uitgevoerd op het eindstation. In de meeste implementaties van firewalls zijn de rule-setmogelijkheden voor een dergelijke contentscreening beperkt. In dat geval is een proxyserver een beter alternatief.

Bovendien vormt het downloaden van content als uitvoerbare programma's, windows-applicaties als *dialers* et cetera, een risico voor het binnenhalen van niet-geautoriseerde programma's als virussen, *spy-ware* en *backdoors*.

Een goede contentscreening zal ook hierop moeten scannen, en dus een vergelijkbare functionaliteit op het systeem moeten hebben, bijvoorbeeld virusscanning. Wat niet in het systeem komt, hoeft er later ook niet af.

Intelligente systemen gebruiken voor contentfiltering een aantal intelligente regels – Baysian, kenmerken, soort pagina, soort URL – eventueel in combinatie met een black list en/of white list. Het is bijvoorbeeld mogelijk om op www.hotmail.com de privémail te lezen en tegelijkertijd te verbieden dat vanaf deze webmailserver bijlagen van een e-mailbericht worden gehaald of verstuurd.

4.4 Overige firewall-functies

4.4.1 Authenticatie

Een belangrijke functionaliteit die de meeste firewalls bieden is authenticatie. Waar een firewall bepaald verkeer zonder expliciete gebruikersvalidatie doorlaat (indien dat in de *rulebase* is geconfigureerd), zijn er scenario's waarbij een gebruiker zich voor bepaald netwerkverkeer expliciet moet aanmelden. Overigens bestaan er ook authenticatiemechanismen voor verkeer dat niet gebonden is aan specifieke gebruikers, bijvoorbeeld VPN-tunnels tussen firewalls, zie figuur 4.9.

Figuur 4.9 Authenticatie

Met betrekking tot authenticatie kan een onderscheid gemaakt worden tussen intrinsieke en additionele authenticatie. Intrinsieke authenticatie is besloten in het applicatieprotocol. Daarbij gaat het bijvoorbeeld om HTTPS, Secure TELNET en Secure FTP. Additionele authenticatie heeft betrekking op protocollen waarin geen intrinsieke mechanismen aanwezig zijn.

Application Level Firewalls kunnen de authenticatie veelal regelen binnen het protocol. Zo kan een HTTP-proxyfirewall een HTTP-aanvraag valideren en na succesvolle authenticatie de communicatie met de feitelijke webserver toestaan. Dit levert een aantal voordelen op boven authenticatie op de applicatieserver. Een firewall kan dan gebruik maken van een centrale gebruikersdatabase voor validatie, zoals een RADIUS- of LDAP-omgeving. Daarnaast kan op gecentraliseerde wijze gebruik worden gemaakt van *Smart Card*-oplossingen.

Wanneer er geen specifieke applicatie-proxycomponent voor een bepaald applicatieprotocol aanwezig is binnen de firewall, of het protocol ondersteunt geen intrinsieke authenticatiemechanismen, dan bieden veel firewalls een eigen oplossing in de vorm van speciale software die geïnstalleerd dient te worden. Zodra de gebruiker een applicatie opstart die met dat bepaalde protocol door de firewall dient te communiceren, dan zal de client automatisch een authenticatie-aanvraag genereren.

4.4.2 Address Translation

In de meeste bedrijfsnetwerken zullen niet alle systemen op internet routeerbare adressen hebben. De meeste netwerken zullen intern zogenaamde RFC 1918-adressen gebruiken (10.0.0.0/8, 172.16.0.0/12 tot 172.32.0.0/12, 192.168.0.0/16). Deze adressen zijn door de IANA gereserveerd voor intern gebruik, en worden niet geaccepteerd door een Internet Service Provider, en zeker niet gecirculeerd op het internet.

Om systemen met een adres uit een van deze reeksen toch te gebruiken voor communicatie over het internet, moet het interne adres vertaald worden naar een adres dat geschikt is voor internet. Er zijn twee technieken die hiervoor gebruikt kunnen worden: *Netwerk Address Translation* en het gebruik van een dual homed proxyserver (zie paragraaf 4.3).

Er zijn drie varianten van Netwerk Address Translation:
- PAT: *Port Address Translation*;
- *Port Forwarding*;
- NAT: Network Address Translation.

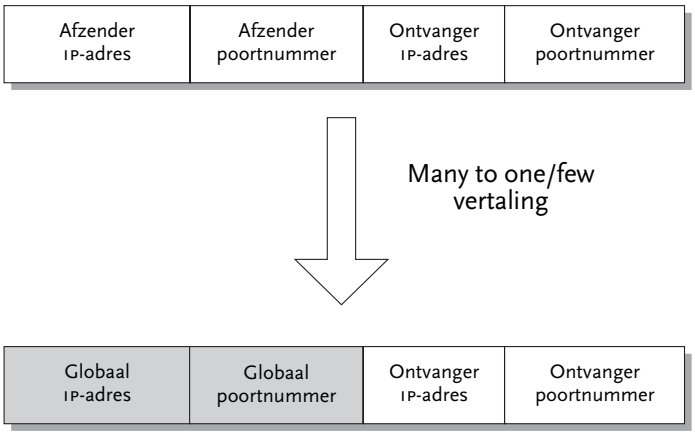
PAT is het vertalen van het afzender-IP-adres en het TCP-poortnummer. Dit vindt plaats op laag 4 van het OSI-model (veel-naar-één-vertaling).

Port Forwarding is het vertalen van het ontvanger-IP-adres en het TCP-poortnummer. Dit vindt plaats op laag 4 van het OSI-model (één-naar-veel-vertaling).

NAT is het vertalen van het afzender- of ontvanger-IP-adres. Dit vindt plaats op laag 3 van het OSI-model (één-op-één-vertaling).

Port Address Translation

Om interne systemen gebruik te laten maken van internetservices moet het interne IP-adres vertaald worden. De meest gebruikte techniek voor zo'n vertaling is Port Adress Translation (PAT), een veel-naar-één-vertaling. Om de veel-naar-één-vertaling mogelijk te maken verandert de firewall niet alleen het afzenderadres, maar ook het afzender-TCP-poortnummer. Zie figuur 4.10.

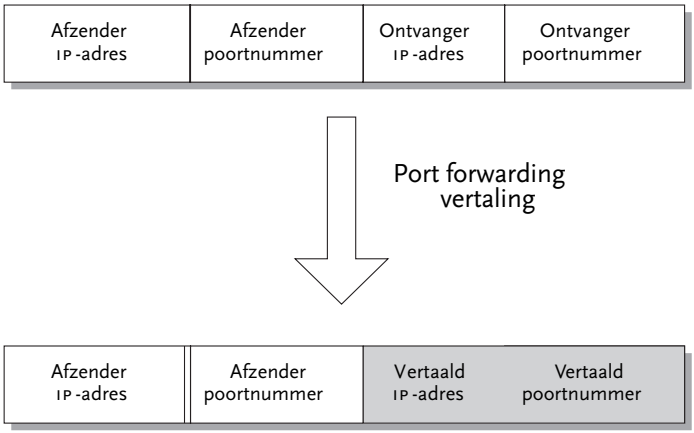


Figuur 4.10 Port Address Translation

Door een tabel bij te houden waarin staat welk poortnummer bij welke connectie hoort, kan er toch een twee-wegcommunicatie worden opgebouwd. Voorwaarde van deze vertaling is dat de sessies vanaf één kant opgebouwd moeten worden. In deze vertaling kan meer dan één IP-adres worden gebruikt, daarom de naam 'veel-naar-één-vertaling'. Het principe blijft dan gelijk. Deze translatie kan niet worden gebruikt om vanaf internet connectie met interne systemen te bewerkstelligen.

Hoewel PAT niet als een echte beveiligingsmaatregel kan worden gezien, beschermt het in zekere mate wel de interne systemen, en zorgt deze vorm van Network Address Translation wel voor het verbergen van de interne structuur van het netwerk. Doordat de interne adressen niet zichtbaar zijn voor de buitenwereld kan er vanuit die buitenwereld ook geen connectie worden opgezet naar specifieke systemen op het interne netwerk. En hoewel dit in de meeste gevallen ook het verlangde resultaat is, is er ook een aantal toepassingen te noemen dat hierdoor niet meer zal functioneren. Denk hierbij vooral aan Streaming- en Real Time-protocollen.

Om toch interne servers vanaf internet te kunnen benaderen, zonder voor iedere service een officieel IP-adres te gebruiken, kunnen twee andere technieken worden gebruikt: Port Forwarding en NAT.



Figuur 4.11 Port Forwarding

Port Forwarding

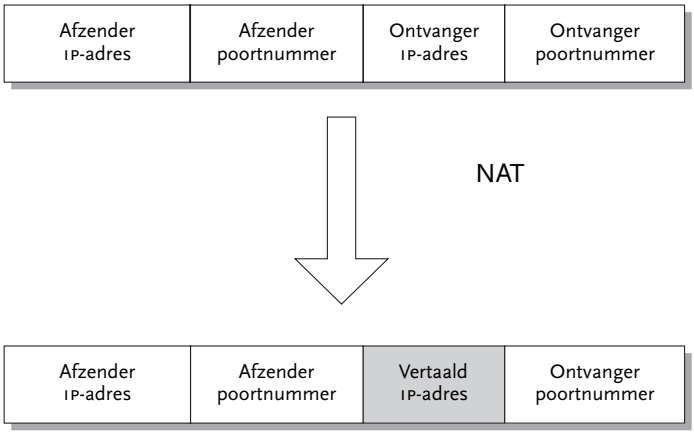
Met behulp van Port Forwarding, zie figuur 4.11, kan verkeer dat bijvoorbeeld op de internetinterface van de firewall binnenkomt op poort 80 (dus voor een webserver) worden doorgestuurd naar een webserver ergens op het interne netwerk, met een intern adres, en verkeer op poort 110 (POP3) naar een andere server.

Wederom blijft de interne structuur van het netwerk verborgen, en zal er geen verkeer vanaf de firewall naar de interne server mogelijk zijn, anders dan in de Port Forwarding-regels is vastgelegd.

Network Address Translation

Met behulp van Network Adress Translation (NAT), zie figuur 4.12, worden alleen de IP-adressen van de ontvanger of afzender gewijzigd. Deze vertaling zal altijd één-op-één zijn. Hierdoor is voor elk systeem dat vanaf een extern netwerk bereikbaar moet zijn ook een extern IP-adres nodig. Er vindt dus een één-op-één-vertaling plaats.

Hoewel services als PAT/NAT/port forwarding veel gebruikt worden, geven verschillende protocollen ook problemen indien ze gebruikt worden in combinatie met deze services. Hoofdoorzaak hiervan is dat de



Figuur 4.12 Network Address Translation

protocollen het afzenderadres ook in de data van het pakket hebben staan, en dus na vertaling twee verschillende adressen hebben, één in de header en één in de payload.

4.4.3 Routeren

De firewall en de router zijn twee van de meest voorkomende perimetercomponenten. Het zijn tevens twee veiligheidscomponenten die op gemeenschappelijke basis kunnen worden ingezet in een firewall-architectuur. De primaire routerfunctionaliteit wordt dan gecombineerd met een beperkte filterfunctie om aan de rand van het netwerk bepaald ruisverkeer (onnodige datapakketten, bijvoorbeeld broadcastverkeer) af te stoten, waarvan we de resultaten niet willen terugzien in de firewall-*logging*. Door deze filtering wordt de firewall tevens ontlast. Daarnaast kan de router inspelen op gevaarlijke routeringsopties alsmede op in- en uitgaand ICMP-verkeer. Door de routerfiltering zo veel mogelijk te beperken, komt het *overall*-beeld met betrekking tot het toegestaan en geblokkeerd verkeer hoofdzakelijk uit de firewall-logging.

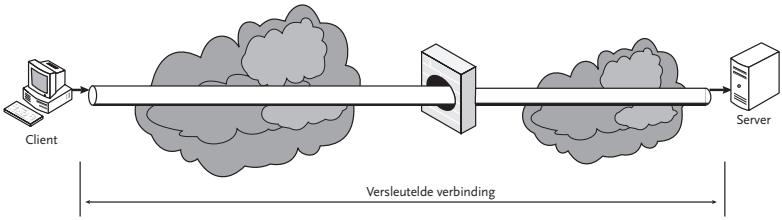
4.4.4 Encryptie

Encryptie, het versleutelen van gegevens zodat deze onleesbaar zijn voor onbevoegden, heeft een lange historie. De Romeinen kenden al methodes om tekst te versleutelen door aan de letters uit het alfabet bepaalde tekens toe te kennen en deze te verschuiven. Ook de Enigma-encryptiemachine is een bekend voorbeeld.

Encryptie is tegenwoordig de basis van technologieën als IPsec, VPN en SSL. Er is een grote opkomst van VPN-verbindingen, thuiswerkers maken er bijvoorbeeld steeds vaker gebruik van, net als kantoren die via internet met elkaar verbonden willen zijn zonder daarvoor de kosten van een directe lijn te willen dragen. De SSL-technologie wordt veelvuldig toegepast bij het beveiligen van webverkeer (HTTPS) of diverse mail- en directoryprotocollen (POP3, IMAP4, LDAP).

De gebruikte encryptiemechanismen zijn van groot belang voor de firewall-infrastructuur. Een belangrijke keuze die gemaakt moet worden is waar het eindpunt binnen het bedrijfsnetwerk wordt gelegd voor dergelijke versleutelde verbindingen. In principe zijn er drie mogelijkheden.

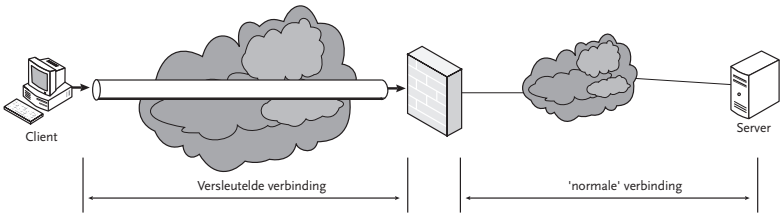
Allereerst kan de versleutelde verbinding worden getermineerd op een speciale component. Daarbij gaat het om bijvoorbeeld VPN-*concentrators* of SSL-*offloaders*. Vaak wordt deze mogelijkheid gebruikt bij versleutelde tunnels (*multipoint-to-multipoint*-verbindingen). Wanneer deze componenten binnen het bedrijfsnetwerk staan, is het belangrijk in te zien dat het verkeer niet door de firewall geïnspecteerd kan worden (het is tenslotte versleuteld). Alleen het opzetten van een VPN (de sessie-opbouw) kan door de firewall gecontroleerd worden, maar als de verbinding eenmaal is toegestaan, is er geen controle op de inhoud meer mogelijk. Zie figuur 4.13. Een eventuele Application Level Firewall moet op dat moment in pakketfilteringmodus gaan werken. Wanneer de componenten echter vóór de firewall staan (of in een DMZ tussen twee firewalls) kan na ontsleuteling wel een controle op applicatieniveau worden bewerkstelligd.



Figuur 4.13 Encryptie *end to end*

De versleutelde verbinding kan ook getermineerd worden op een host. Hierbij gaat het veelal om een point-to-point-verbinding, bijvoorbeeld een browserverbinding naar een SSL-*enabled* webserver. De encryptieprocessen vinden dan plaats op de host, waardoor de firewall het verkeer niet kan inspecteren. De firewall fungeert slechts als een pakketfilter.

Ten slotte is termineren op de firewall zelf ook een mogelijkheid. Zie figuur 4.14. De firewall ontsleutelt het inkomend verkeer en kan dit vervolgens inspecteren. Dit betekent echter dat de firewall aanzienlijk meer systeembronnen nodig heeft voor encryptiemechanismen.



Figuur 4.14 Encryptie tot aan de firewall

4.4.5 Virtual Private Network

Firewalls zijn belast met de controle op de toegang tot resources en Virtual Private Networks (VPN's) zorgen voor beveiligde verbindingen tussen hosts en netwerken. Firewalls en VPN's worden om de volgende redenen vaak tezamen besproken:

- Afhankelijk van de netwerkarchitectuur kunnen VPN en NAT niet tegelijk worden toegepast.
- VPN in *tunnel mode* maakt de inspectie van encryptieverkeer lastig voor firewalls.
- VPN-eindpunten hebben toegang tot de data in *clear text*. Daarom moeten de apparaten extra beveiligd worden en bijvoorbeeld achter de firewall worden geplaatst.

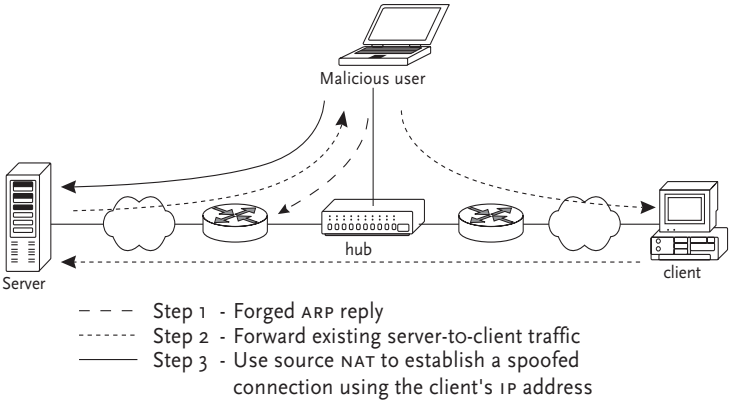
VPN-functies kunnen in de firewall worden geïntegreerd tot één systeem. Dit heeft voor- en nadelen. Een geïntegreerde oplossing is goedkoper ten aanzien van het beheer. Er zijn minder systemen en bepaalde commerciële producten leveren een beheerinterface waarmee het beheer kan worden vereenvoudigd. Daarnaast hebben deze producten geen NAT-gerelateerde problemen en kunnen ze gebruikmaken van de *access-control*-faciliteiten van de firewall. Het grootste nadeel is dat de integratie ten koste kan gaan van de flexibiliteit. Met losse componenten kan veel

meer maatwerk worden geleverd ten opzichte van gecombineerde *business/security requirements* dan met een geïntegreerde oplossing.

4.4.6 Antispoofing

De basis van de spoofing-techniek bestaat uit het gericht afschermen of veranderen van de eigen identiteit bij het verzenden van berichten. Binnen het kader van de IT-beveiliging bestaan vele vormen van spoofing, voorbeelden zijn IP-spoofing en webspoofing. IP-spoofing is de meest voorkomende techniek en een belangrijke component van een netwerkaanval; het is de beste wijze van online camouflage. Het concept van IP-spoofing werd rond 1980 voor het eerst gebruikt in combinatie met *TCP sequence number prediction*, om toegang te krijgen tot een netwerk of machine door berichten te verzenden met een gespooft afzender-IP-adres van een vertrouwde machine.

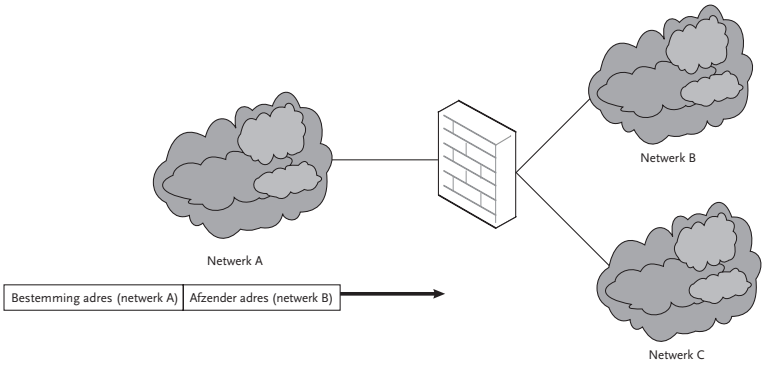
Door de verbetering van de TCP/IP-stack komt dit soort aanvallen minder voor, echter, IP-spoofing wordt nog wel op grote schaal toegepast bij technieken als *man-in-the-middle*, *routing redirects*, *denial-of-service* en *blind spoofing*. Een schematisch voorbeeld van een man-in-the-middle-aanval is in figuur 4.15 weergegeven.



Figuur 4.15 Man-in-the-middle-aanval met behulp van spoofing

Bij IP-spoofing wordt het adres van de verzendende machine vervangen door een ander adres, waarmee de (IP-)identiteit van de zender wordt afgeschermd. Hierbij bestaat echter vaak de misvatting dat IP-spoofing gebruikt zou kunnen worden als middel om anoniem te kunnen communiceren over netwerken. Dit is niet het geval; de antwoordpakketten zullen immers niet aankomen bij de originele zender, maar bij de host die het feitelijke (gespoofte) IP-adres bevat.

De meeste firewall-systemen bevatten mechanismen om IP-spoofing tegen te gaan. De belangrijkste zijn ACL's (Access Control Lists) op de interfaces van de firewall. Deze zijn zo geconfigureerd dat er gecontroleerd wordt of het afzenderadres in overeenstemming is met het netwerk waar het pakket vandaan komt of naar toe gericht is. Een pakket dat vanaf internet de firewall bereikt, mag dan geen afzenderadres bevatten dat tot een van de interne (private) netwerken behoort. Evenzo moet een pakket dat gericht is aan internet een afzenderadres bevatten dat behoort tot een van de (bekende) interne netwerken. In figuur 4.16 wordt een situatie weergegeven waarin de firewall het gespoofte pakket niet accepteert, doordat het pakket met het gespoofte afzenderadres van netwerk B aankomt op een interface die gekoppeld is aan netwerk A.
Andere mechanismen om IP-spoofing tegen te gaan, zijn gebaseerd op het gebruik van protocolencryptie en authenticatie. Deze mechanismen vergen echter aanpassingen die niet gemakkelijk op grote schaal of op publieke netwerken door te voeren zijn.



Figuur 4.16 Smartspoof

Concluderend kan worden gesteld dat IP-spoofing een probleem is waarvoor geen eenvoudige oplossing bestaat, doordat een deel van de werking inherent is aan het functioneren van de TCP/IP-stack. De meeste firewalls hebben echter anti-spoofingcomponenten ingebouwd. Bij het configureren van antispoofing moet men erop letten dat het overige netwerkverkeer niet wordt beïnvloed.

4.4.7 Intrusion detection

In deze paragraaf wordt beschreven wat *intrusion detection* inhoudt en hoe de relatie tot het gebruik van firewalls is.

De praktijk leert ons dat er incidenten voorkomen waarbij niet toegestaan netwerkverkeer toch plaatsvindt achter de firewall (die dus dat netwerkverkeer geblokkeerd zou moeten hebben). Dit wordt in deze studie 'inbraak' genoemd. Een dergelijke inbraak zal opgemerkt of gedetecteerd moeten worden door apparatuur en programmatuur die het netwerkverkeer constant monitoren. Dit is het concept van *intrusion detection*.

Indien een inbraak opgemerkt wordt, zal deze geregistreerd moeten worden (logging/alerting) waarna een reactie zal moeten komen. Deze reactie kan zowel automatisch als na menselijke beoordeling gegeven worden.

Het is mogelijk dat een *intrusion detection system* (IDS) autonoom actie onderneemt om de inbraak te corrigeren (bijvoorbeeld door de rule set van de firewall aan te passen). Op dat moment wordt er gesproken van een *intrusion prevention system* (IPS). IPS voorkomt of blokkeert een aanval. De reactiesnelheid van dergelijke systemen is erg belangrijk. Hoe sneller gereageerd en gecorrigeerd wordt, hoe meer het een intrusion prevention system zal worden in plaats van een intrusion detection system.

4.4.8 Logging, alerting en reporting

Een gedegen firewall-omgeving voorziet in het genereren van accurate *logfiles*. Logfiles binnen een firewall-omgeving zijn in eerste instantie belangrijk voor de continuïteit van de firewall-functionaliteit. Daarnaast dienen logfiledata voor beveiligingsgerelateerde zaken als het detecteren van pogingen tot compromittering, of het analyseren c.q. verbeteren van de firewall-configuratie. Ten slotte kunnen logfiledata een belangrijke input vormen voor intrusion detection systems, die geautomatiseerde controles uitvoeren op succesvolle en mislukte aanvallen op het netwerk. Voor het invullen van deze functies dienen logfiles informatie te verstrekken over de volgende drie categorieën:

1 kritieke systeemproblemen: hard- en software falen waardoor de firewall niet meer functioneert;
2 administratieve gebeurtenissen: geautoriseerde acties zoals wijzigingen van firewall-rulebase, systeemconfiguratie en account(autorisatie);

Figuur 4.17 Voorbeeld logberichten

3 netwerkverbindingen: verbindingen die geaccepteerd of geweigerd worden, afwijkende verbindingsaanvragen, enzovoorts.

Logging door middel van logfiles, zie figuur 4.17, wordt meestal gegenereerd door de firewall zelf. Het gaat bij deze vorm van logging om gedetailleerde informatie ten aanzien van het opzetten van netwerkverbindingen (*accept*, *reject*, *drop*), het gebruik van bepaalde protocollen en het gebruik van authenticatie- of autorisatiemechanismen (geslaagde of mislukte aanmeldingspogingen).

Het volledige terrein van logging dat relevant is voor een firewall-omgeving, reikt verder dan alleen de logfiles die de firewall-component genereert. Het is daarbij belangrijk dat de data uit de verschillende logfiles geinterpreteerd kunnen worden, in ieder geval de tijd, zodat bepaalde gebeurtenissen duidelijk herleid kunnen worden. Een logsysteem dient zorgvuldig ontworpen te worden om daadwerkelijk relevante informatie te kunnen leveren. Belangrijke punten bij het ontwerp zijn:

- De locatie van de logfiles (op de firewall of via een *remote logging service*): in principe heeft een remote logging service de voorkeur, omdat alle logfiles dan op een centrale plaats opgeslagen en verwerkt kunnen worden. Er dient echter wel rekening gehouden te worden met de beveiliging van de logfileverbindingen en met de beschikbare bandbreedte.
- De verwachte grootte van de logfiles: de opslagcapaciteit mag nooit een beperkende factor zijn voor voldoende logging.
- De snelheid waarmee data worden gelogd: het logfilesysteem moet in staat zijn logfiledata voldoende snel te kunnen verwerken. Meetpunten overslaan door verwerkingsvertraging is onacceptabel.
- De vraag: wie heeft toegang tot de logfiles en wat is het autorisatieniveau? Logfiledata kunnen gevoelige informatie bevatten en moet dus onderworpen zijn aan een beveiligingsprocedure en aan authenticatie- en autorisatiemechanismen. Daarbij is met name het verschil tussen lees- en wijzigingsrechten van belang. Om grote hoeveelheden data (de betere firewall-componenten genereren zeer veel data) te kunnen analyseren, zijn logfiletools beschikbaar waarmee bepaalde filters en analysetechnieken toegepast kunnen worden.
- De vraag: moeten logfiledata versleuteld worden? Hierbij is de overhead bij versleuteling van data van groot belang.

– De vraag: wat is het *backup*- en *recovery*-model voor logfiles? Logfiledata moeten veiliggesteld kunnen worden voor langere termijn, zeker voor eventueel onderzoek bij geconstateerde beveiligingsproblemen.

Reporting

Er zijn tal van commerciële analysetools die ondersteuning bieden bij het beheren, rapporteren en monitoren van firewall-activiteiten, al dan niet in *real-time*. Deze tools analyseren de logbestanden van de firewall en rapporteren onder andere binnenkomende en uitgaande activiteiten, de gebruikte protocollen, wie de protocollen gebruikt, bandbreedte per protocol, mogelijke hack-aanvallen, ongeoorloofd internetgebruik en de hoeveelheid e-mail die verstuurd en ontvangen wordt. Een belangrijk aandachtspunt bij *reporting* is de vertrouwelijkheid van de informatie waarover gerapporteerd wordt.

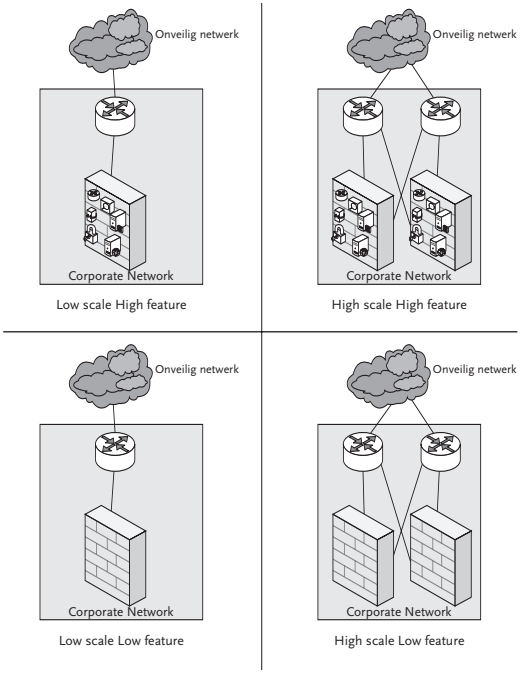
5 Ontwerpcriteria voor een firewall

5.1 Inleiding

Als een firewall het antwoord is, wat was dan de vraag?

Wat beweegt een organisatie om in een specifieke situatie te kiezen voor een bepaalde verschijningsvorm van een firewall? Wat zijn eigenlijk de criteria die de firewall-configuratie, evenals het ontwerp waarvan de firewall-configuratie deel uitmaakt, bepalen?
Figuur 5.1 toont ter illustratie een aantal mogelijke verschijningsvormen van een firewall-configuratie. In dit voorbeeld is een van de verschillen tussen de verschillende firewalls het al dan niet aanwezig zijn van extra beveiligingsfuncties. Schaalbaarheid, *load balancing* en redundantie zijn andere mogelijke verschillen. Voor een overzicht van de verschillende eigenschappen van een firewall wordt verwezen naar tabel 5.1.

Uit een studie van FBI en CSI (*FBI/CSI Computer Crime and Security Survey 2004*) blijkt dat 98 procent van de respondenten een firewall gebruikt. Op voorhand zijn er geen redenen te bedenken waarvoor dit in Nederland beduidend anders zou zijn. Ons uitgangspunt is dan ook dat in elke organisatie een firewall aanwezig is, die deel uitmaakt van de basisvoorzieningen op het gebied van informatiebeveiliging. Kortom: een firewall is het antwoord op een duidelijke behoefte. De studie *Firewalls* gaat in op de rol van een firewall, op de positie van een firewall in het totale pakket van beveiligingsmaatregelen, op de waarde en op de plaats van een firewall in een beveiligingsarchitectuur.

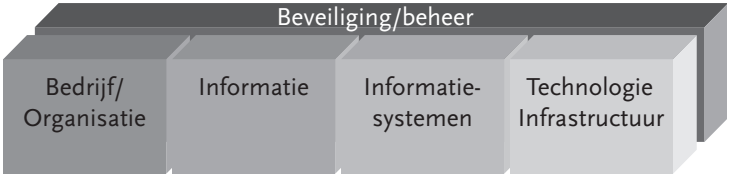


Figuur 5.1 Verschijningsvormen van een firewall-configuratie

Er kunnen ontwerpcriteria voor een firewall opgesteld worden. Deze criteria zijn relevant voor bijvoorbeeld de volgende situaties:

- het opstellen van selectiecriteria bij aankoop van firewalls of firewall-services;
- het controleerbaar vaststellen van een wenselijk beveiligingsniveau;
- het beveiligingsniveau laten voldoen aan eisen en richtlijnen van regelgevende of toetsende (externe) instanties die een overzicht vereisen van de geboden beveiliging, waarbij de nadruk ligt op de evenwichtigheid;
- het afsplitsen van een bedrijfsonderdeel door verkoop of *outsourcing*.

Het beveiligen van een IT-omgeving is een complexe taak. Beveiliging heeft niet alleen met techniek te maken maar ook met de organisatie, het informatiebeleid, de cultuur, de wetgeving, de al in gebruik zijnde apparatuur, de financiën, de ontwikkelingen op de markt, de procedures, et cetera. Zie figuur 5.2.



Figuur 5.2 Verschillende aspectgebieden van beveiliging

Een ontwerp moet antwoord geven op de vragen wat, waarom en waartegen beveiligd moet worden. Met een ontwerp kunnen we dan antwoord geven hoe, op welke wijze, waarmee en eventueel ook wanneer beveiliging gerealiseerd kan worden.

5.2 Firewall als een component van de fysieke IT-infrastructuur

De fysieke architectuur geeft aan waarmee een oplossing gerealiseerd wordt, met welke componenten en in welke constellatie.

Waar vroeger afhankelijk van noodzaak overwogen werd een firewall toe te voegen aan een bestaande of te ontwerpen infrastructuur, is de firewall tegenwoordig een standaardcomponent in elke infrastructuur.

De firewall als beveiligingscomponent werkt alleen indien deze op de juiste wijze gekoppeld is en samenwerkt met de overige componenten waaruit de IT-infrastructuur bestaat. Een firewall is een beveiligingsmaatregel, die als filterende netwerkkoppeling wordt ingezet. Inzet van een firewall vraagt ook om aanvullende beveiligingsmaatregelen, met name om inrichting van het operationele beheer.

De vraag blijft: welke firewall-oplossing te kiezen? Of liever gezegd: welke set van functionaliteiten (zoals beschreven in hoofdstuk 4) te kiezen en hoe deze te implementeren en te configureren?

Tabel 5.1 Voorbeeld van karakteristieken van een firewall

Karakteristiek	Eis	Detailontwerp
Beschikbaarheid	Standaard: bijvoorbeeld 98%	Alle componenten enkelvoudig uitgerust – servicecontracten
	Hoog: bijvoorbeeld 99%	Alle componenten redundant uitgerust, backup & recovery van ieder component mogelijk binnen twee uur
	Zeer hoog: bijvoorbeeld 99,5%	Alle componenten redundant uitgevoerd met een directe overname van de functionaliteit door de overblijvende systemen in geval van uitval (Hot stand-by/Stateful failover)
Kwaliteit van de bewaking van de communicatiematrix (inverse van hackbaarheid)	Normaal	Enkelvoudige firewalltechnologie Packet filtering (statisch/dynamisch)
	Hoog	Dubbele firewalltechnologie (firewalls van twee verschillende leveranciers achter elkaar) Hybride (stateful) inspectiefiltering
Beheerbaarheid	Normaal	Alles geïntegreerd binnen centrale managementsystemen
	Hoog (lage operationele kosten)	Oplossing op basis van één enkele leverancier; standaardisatie
Controleerbaarheid	Normaal	Regelmatige Log-analyse van essentiële netwerkcomponenten
	Hoog	Specifieke Intrusie Detectie Systemen voor het netwerk en de serversystemen
Schaalbaarheid	Normaal	Gebruikte systemen hebben in initiële versie x% overcapaciteit – als de groei daarboven komt, moet het systeem vervangen worden door een systeem met meer capaciteit
	Hoog	Componenten zodanig kiezen dat extra capaciteit toegevoegd kan worden door extra componenten bij te plaatsen (n+1 architectuur) of door extra modules in een systeem te plaatsen (bijvoorbeeld extra CPU's of geheugen)

Karakteristiek	Eis	Detailontwerp
Integriteit	Normaal	Bewaking via analyse firewall logging-bestanden en alarmering op basis van specifieke gebeurtenissen Toegangscontrolesysteem op basis van passen
	Hoog	Separaat Intrusie Detectie Systeem voor het monitoren van verdachte gebeurtenissen op het netwerk en/of op de serversystemen Toegangscontrole op basis van biometrie
Latentie	Normaal	Noodzakelijke filteringmechanismen kunnen zonder probleem worden toegepast
	Laag en ondersteuning real time en streaming protocollen	Hybride en dynamische filtering nauwelijks mogelijk door latentie en jitter over de firewalls. Additionele routering en aanvullende Source Authenticatie en autorisatie nodig

5.3 Ontwerpmethodiek

Inleiding ontwerpmethodiek

In dit hoofdstuk wordt een aanzet gegeven om op basis van enkele kenmerken aan te geven welke maatregelen minimaal nodig zijn voor een basisbeveiligingsniveau. Het geeft de achterliggende gedachten weer die tot een oplossing leiden. Het is noodzakelijk om alle stappen op de beschreven wijze uit te voeren. Dat betekent niet dat er slechts één oplossing voor het ontwerp van een firewall bestaat, maar het is van belang dat alle relevante factoren worden beoordeeld. Door de methode toe te passen kan op basis van de eigen omgeving een hoger of lager niveau van beveiliging worden gecreëerd.

In het ontwerpproces voor een firewall maken we gebruik van de top-downbenadering. De top-downbenadering is een aanpak waarbij eerst op hoog niveau naar de vereisten wordt gekeken en dan langzaam wordt afgedaald tot het niveau waarop de daadwerkelijke implementatie plaatsvindt. Iedere stap volgt uit de vorige stap en is daarom een verdieping

van de vorige stap. Voor een (kosten)effectief ontwerp is het verstandig om ook aspecten uit de bottom-upbenadering mee te nemen. In deze benadering komen de middelen die beschikbaar zijn en de mogelijkheden die men heeft, aan bod.

Het ontwerpproces van een firewall-systeem:

1 analyse van de situatie en de eisen aan de oplossing:
   a inventarisatie van business-eisen, wet- en regelgeving, informatiebeveiligingsbeleid;
   b inventarisatie van de domeinen;
   c data- en systeemclassificatie;
   d risicoanalyse;
   e inventarisatie van de bestaande middelen;
2 logisch ontwerp:
   a datastromen;
   b selectie van 'filterende' maatregelen;
3 functioneel ontwerp:
   a fysieke elementen;
   b wenselijkheid;
   c haalbaarheid;
4 analyse van verschillen tussen gewenste en huidige situatie (gap-analyse);
5 implementatie;
6 evaluatie.

De bovenstaande punten moeten allemaal worden uitgewerkt om ook later te kunnen rechtvaardigen waarom er tot een keuze gekomen is, welke risico's er genomen zijn en wie deze risico's heeft aanvaard. Het gaat er niet alleen om de gekozen oplossing te beschrijven en te onderbouwen, maar vooral ook om de zaken die niet zijn bekeken of bewust zijn weggelaten, te documenteren.

Ontwerpstappen

We zullen in de volgende paragrafen de stappen doornemen. Voor elk van de stappen zullen we laten zien welke basiskeuzes er gemaakt dienen te worden. Tevens wordt het raamwerk waarbinnen de keuzes moeten worden gemaakt, besproken en wordt er bovendien aangegeven aan welke minimumeisen het ontwerp moet voldoen.

5.3.1 Stap 1: analyse van de situatie en eisen aan de oplossing

De inventarisatie van de vereisten omvat de volgende activiteiten:
a inventarisatie van business-eisen, wet- en regelgeving, informatiebeveiligingsbeleid;
b inventarisatie van de domeinen;
c data- en systeemclassificatie;
d risicoanalyse;
e inventarisatie van de bestaande middelen.

Voordat we een ontwerp kunnen maken aan de hand van de in deze studie opgestelde criteria, moet eerst gekeken worden naar de vrijheden en beperkingen. Deze worden bepaald door de opgelegde eisen. De eisen komen voort uit de bedrijfsvoering en worden vertaald in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Een leidraad is het Informatiebeveiligingsbeleid. Dit beleid zou ook rekening moeten houden met de regelgeving van de branche waarin de business opereert en moeten voldoen aan de wetten.

In de volgende stap van het ontwerp gaan we bekijken welke domeinen een rol spelen in de omgeving. De te kiezen beveiligingsmaatregelen zijn zeer sterk afhankelijk van deze domeinen.

Om alles inzichtelijk te maken, maken we gebruik van een vertrouwensmatrix. In deze matrix wordt het vertrouwensniveau van de verschillende soorten domeinen (meestal ook netwerken) geclassificeerd om daarna bij het koppelen van de domeinen te kunnen bepalen welke maatregelen er minimaal nodig zijn. Hiervoor worden de verschillende koppelingen elk afzonderlijk beschouwd.

Om te bepalen of, en zo ja in hoeverre, er sprake is van te vertrouwen netwerken en domeinen, kan voor het uitvoeren van de risicoanalyse gebruik worden gemaakt van een schema, een zogeheten vertrouwensmatrix. Uitgangspunt is dat het eigen beheer altijd plaatsvindt conform de interne richtlijnen en voldoet aan de gestelde beheer- en beveiligingseisen. Dat geldt zowel voor de netwerkdiensten als voor het beheer van de overige componenten. De vertrouwensmatrix heeft ten doel het ver-

trouwensniveau van een netwerkdomein vast te stellen. Een netwerkdomein bestaat uit systemen (servers en clients) en het netwerk. We onderscheiden drie soorten netwerken en drie soorten systemen. Deze onderverdeling levert een matrix op met negen cellen, zie figuur 5.3.

Netwerk / Systemen	Eigen beheer	Gedelegeerd beheer	Onbekend
Eigen beheer	Vertrouwd	Deels vertrouwd	Onvertrouwd
Gedelegeerd beheer	Deels vertrouwd	Deels vertrouwd	Onvertrouwd
Onbekend	Onvertrouwd	Onvertrouwd	Onvertrouwd

Figuur 5.3 Vertrouwensmatrix

Toelichting vertrouwensmatrix

Uit de matrix is af te leiden dat we slechts één domein echt als vertrouwd kunnen aanmerken, namelijk een domein waarin we zowel het netwerk als de systemen zelf beheren, de eigen systemen en netwerken. Als er sprake is van een domein waarbinnen onbekende componenten voorkomen, is dit een onvertrouwd domein, zelfs al bevinden zich ook zelf beheerde componenten in dat domein. Daar waar uitbestede componenten voorkomen, of gecontroleerde diensten zijn afgenomen (waarbij contractuele afspraken over het beveiligingsniveau zijn gemaakt), kan sprake zijn van een deels vertrouwd domein.

Voor elk van de betrokken domeinen wordt de vertrouwensmatrix ingevuld. Daarbij wordt het te beveiligen domein, waarvan de eigenaar zelf de policy bepaalt, als uitgangspunt genomen.

Het resultaat van de eerste fase is een beschrijving van de verschillende domeinen waarop de firewall-architectuur betrekking heeft. Deze omschrijving bevat een classificatie van de domeinen, een analyse van de verschillen en een analyse van de risico's. Dit zijn de basiselementen die in de vervolgstappen gebruikt worden om keuzes te rechtvaardigen.

5.3.2 Stap 2: opstellen logisch ontwerp

In het logisch ontwerp worden op basis van de geïdentificeerde datastromen de noodzakelijke filterende maatregelen geselecteerd.

Allereerst zullen de datastromen in kaart moeten worden gebracht. Tussen welke domeinen is communicatie nodig en wat houdt deze communicatie in? Een interessant fenomeen is een koppeling die door een ander domein heenloopt. Een voorbeeld is een koppeling van een laptop aan een bedrijfsnetwerk via internet.

Als de datastromen bekend zijn, kunnen de te gebruiken filterende maatregelen geselecteerd worden. De maatregelenmatrix kan hierbij hulp bieden. Deze matrix geeft aan welke maatregelen er minimaal moeten worden genomen voor koppelingen tussen twee domeintypen (zoals die met behulp van de vertrouwensmatrix in de voorgaande paragraaf werden bepaald). Zie figuur 5.4.

Maatregelen / Koppelen domeinen	Pakket-inspectie	Applicatie-inspectie		Intrusion detection	Encryptie	DMZ
		Proxy	Content screening		VPN	
Onvertrouwd → vertrouwd	✓	✓	✓	✓		✓
Vertrouwd → onvertrouwd	✓	✓				✓
Deels vertrouwd → vertrouwd	✓	✓		✓		✓
Vertrouwd → deels vertrouwd	✓	✓				✓
Vertrouwd domein x → vertrouwd domein x via onvertrouwd domein					✓	
Vertrouwd domein (hoog beveiligingsniveau) koppelen met domein met lager niveau	✓	✓	✓	✓		
Vertrouwd domein (laag beveiligingsniveau) koppelen met domein met hoger niveau	✓					

Figuur 5.4 Maatregelenmatrix

Toelichting maatregelenmatrix

In de eerste kolom van de maatregelenmatrix staan de verschillende soorten netwerkkoppelingen. Daarbij zijn de verschillende netwerken ingedeeld conform de vertrouwensmatrix. In de volgende kolommen staan de te treffen beveiligingsmaatregelen. Een DMZ is echter geen beveiligingsfunctie van een firewall, maar een ontwerpprincipe. Gezien zijn belang is dit principe wel in de matrix opgenomen. De in hoofdstuk 4 opgevoerde standaardfuncties als logging en alerting, adresvertaling, authenticatie en anti-IP-spoofing staan niet in het overzicht, omdat deze functies in elke situatie zullen voorkomen.

Korte toelichting op de kolommen (zie ook hoofdstuk 4)

- Pakketinspectie: een beperkte beveiligingsfunctie, gericht op netwerkbeveiliging in enge zin, OSI-lagen 2,3 en 4, netwerkaanvallen. In de meeste gevallen wordt deze functie vervuld door een router.
- Proxy: in hoofdstuk 4 zijn verschillende soorten proxyfilters beschreven. De keuze van het soort filter hangt af van verschillende afwegingen. Daarop komen we later terug.
- Contentscreening: een filterfunctie die op basis van het gedefinieerde beveiligingsbeleid de daadwerkelijke inhoud van de communicatie beoordeelt. Te denken valt aan virusscanners en URL-blokkering door black lists.
- Intrusion detection: inbraakdetectie en -preventie kunnen op verschillende plekken worden toegepast. In dit overzicht beperken we ons tot het vaststellen van de noodzaak binnen het firewall-ontwerp. Aangezien IDS/IPS evenals loganalyse complexe materie is, worden geen ontwerpregels uitgewerkt, dat zou de scope van deze studie te buiten gaan.
- VPN: een vorm van encryptie voor data op transport tussen vertrouwde componenten. Hiermee wordt de authenticiteit van beide componenten gewaarborgd en worden de gegevens versleuteld zodat ze gedurende het transport onleesbaar zijn voor onbevoegden. Een VPN wordt bijvoorbeeld ingericht om over het onvertrouwde internet met een vertrouwde partij gegevens te kunnen uitwisselen.
- DMZ: de plaats waar services in de firewall worden opgesteld. Kenmerk is dat er geen productiegegevens aanwezig mogen zijn in de DMZ. In die zin is een DMZ dan ook geen beveiligingsmaatregel,

maar een ontwerpprincipe. In de regel is een DMZ omsloten door netwerkfilters.

Korte toelichting op de rijen

De rijen van de maatregelenmatrix beschrijven de richtlijnen voor de toepassing van een firewall in een situatie waarin een eigen netwerk (een vertrouwd domein) aan een ander domein wordt gekoppeld. Relevant is daarbij niet alleen het niveau van vertrouwen, maar ook de richting van de communicatie. Daar waar bijvoorbeeld 'onvertrouwd' staat, kan internet worden bedoeld. Een vertrouwd netwerk is bijvoorbeeld een extranet.

Voor andere, meer specifieke situaties kan er gebruik worden gemaakt van de functionaliteitenmatrix. Hierin worden voor specifieke vereiste functionaliteiten uitzonderingen of aanvullingen op de voorgaande ontwerpregels aangegeven. Zie figuur 5.5. Dat kan betekenen dat in vergelijking tot de maatregelenmatrix meer of minder maatregelen gewenst zijn. Elke wijziging moet worden gedocumenteerd en gemotiveerd.

Het kan voorkomen dat er in specifieke situaties voor wordt gekozen om een van de aangegeven filters niet te gebruiken. In dat geval zal minimaal moeten worden onderbouwd waarom deze keuze gemaakt is en welke risico's daaraan verbonden zijn.

Maatregelen / Aard verbinding	Pakket-inspectie	Applicatie-inspectie		Intrusion detection	Encryptie	DMZ
		Proxy	Content screening		VPN	
Publiceren services	✓			✓		✓
Inkomende verkeersstromen	✓	✓	✓	✓		✓
Uitgaande verkeersstromen	✓	✓	✓			
Transit verkeersstromen (niet bestemd voor beschermde domein)	✓				✓	
Vertrouwd domein (hoog niveau) → domein (laag niveau)	✓					

Figuur 5.5 Functionaliteitenmatrix

Dataclassificatie

In de eerste stap is er een classificatie gegeven van de domeinen. Op basis van de classificatie van gegevens en processen zou een hoger of lager niveau van beveiliging kunnen worden gerealiseerd. In specifieke omstandigheden kan het bijvoorbeeld nodig zijn om meer of minder maatregelen te treffen. Het aanbieden van een webservice waarmee vertrouwelijke gegevens beschikbaar worden gesteld, betekent ten opzichte van de keuze in de functionaliteitenmatrix dat meer aanvullende maatregelen nodig zijn in bijvoorbeeld de vorm van versterkte authenticatie en versleuteling.

Deze stap is niet met behulp van een matrix te nemen. Er is een analyse van de te beveiligen omgeving (systemen en processen) en van de eerder vastgestelde maatregelen nodig. Als wordt besloten om op basis van de dataclassificatie af te wijken van de voorgeschreven maatregelen, dan dient dit zeer goed te worden onderbouwd. Bij de keuze voor een lager beveiligingsniveau zal moeten worden aangegeven waarom een lager niveau aanvaardbaar is, bij het toepassen van een hoger niveau zal moeten worden aangegeven wat de rechtvaardiging is van de extra kosten, et cetera.

Logisch ontwerp

Het logisch ontwerp staat los van fysieke beperkingen. De vraag waarop het ontwerp zich concentreert, is immers hoe bepaalde zaken worden uitgevoerd, niet waarmee dit wordt gedaan. Het is van belang meerdere oplossingsrichtingen of -scenario's in het ontwerp te betrekken. Dit stelt de ontwerper en de opdrachtgever in staat om de gevoeligheden en afhankelijkheden van de gekozen oplossing te analyseren. Mogelijke scenario's kunnen bijvoorbeeld zijn:

- toevoegen van nieuwe filialen in een ander land;
- splitsen van de interne organisatie in zelfstandige business-eenheden;
- verwachte groei van het via internetservices afgehandelde deel van de aanvragen van 10 naar 90 procent binnen twee jaar;
- minimaliseren van de investeringen;
- verlagen van de operationele kosten;
- koppelen van laptops via een draadloze netwerkverbinding;
- centraliseren van de beveiligingsoplossing.

Het logisch ontwerp moet helder weergeven wat er gaat gebeuren, zonder dat dit al technisch is uitgewerkt. In logische begrippen en schema's moet duidelijk zijn welke elementen welke rollen gaan spelen.

5.3.2 Stap 3: opstellen functioneel ontwerp

Het opstellen van het functioneel ontwerp hangt sterk samen met het maken van keuzes. Het is zaak om de op grond van de in de voorgaande stappen vereiste functionaliteit in te vullen door de noodzakelijke middelen te specificeren en de procedures te ontwerpen. Verschillende elementen spelen een rol bij het opstellen van het functioneel ontwerp en daarbij kunnen diverse spanningsvelden ontstaan. We onderkennen:
– fysieke elementen;
– wenselijkheid;
– haalbaarheid.

Fysieke elementen

Allereerst moet worden nagegaan aan welke fysieke eisen het ontwerp zal moeten voldoen. Hierbij moet rekening worden gehouden met de eisen in stap 1 en 2, maar ook met de eisen die door de omstandigheden worden opgelegd. Bijvoorbeeld de snelheid van het netwerk of het type aansluiting.

Wenselijkheid

Functionaliteit

Er moet eerst worden nagegaan of de voorgestelde component datgene kan wat ervan verwacht wordt. Dit klinkt logisch, maar helaas gebeurt dit bij de selectie van hardware en software zelden. Het kan ook technisch onmogelijk zijn om uit te voeren wat er wordt gevraagd. Ter verduidelijking gebruiken we in deze paragraaf het voorbeeld van een webserver waarnaar de gebruikers op internet een HTTPS-sessie opzetten. De koppelingenmatrix vereist in deze situatie een proxy. Het proxiën van grote hoeveelheden HTTPS-verkeer behoort (nog) niet tot de mogelijkheden. Dit zal dus niet kunnen worden ingevuld.

Effectiviteit

Er moet ook vastgesteld worden of de voorgestelde oplossing wel de effectiviteit heeft die ervan wordt verwacht. Om terug te komen op het HTTPS-voorbeeld: het toevoegen van intrusion detection aan een firewall die enkel HTTPS-verkeer doorlaat, heeft een erg beperkte toegevoegde waarde. Het kan dan effectiever zijn om de beschikbare middelen op een andere wijze of op een andere plaats in te zetten. Zo kun je intrusion detection aan de server verbinden.

Haalbaarheid

Naast de wenselijkheid van de oplossing moet ook worden nagegaan of de gevraagde oplossing wel haalbaar is. Dat betekent niet alleen nagaan of de oplossing haalbaar is met de aan te schaffen of reeds bestaande middelen, maar ook of zij haalbaar is voor de organisatie qua implementatie en/of beheer.

Beheerorganisaties zijn vaak niet klaar om een intrusion-detection-systeem in beheer te nemen. Een degelijk systeem vraagt veel kennis en tijd. Er zal daarom gekeken moeten worden of de voorgestelde architectuur haalbaar is en er zal moeten worden geanalyseerd waarom bepaalde zaken niet geïmplementeerd kunnen worden. Risicoanalyse ten aanzien van de restrisico's die hierdoor worden gelopen, is een permanente activiteit.

Consequenties

Bij het opstellen van een functioneel ontwerp moet ook goed worden gekeken naar de consequenties voor zowel de organisatie als de kosten. Zoals bekend wordt verondersteld, is er een duidelijk spanningsveld tussen beveiliging en gebruiksmogelijkheden. Te strikte beveiliging maakt het werken onmogelijk, het toestaan van te veel mogelijkheden creëert mogelijk beveiligingsrisico's. Het is dus zaak goed in de gaten te houden wat de gevolgen zijn voor de organisatie en welke risico's de beveiliging met zich meebrengt. Wat betreft de kosten is bijna alles mogelijk, als er maar genoeg middelen beschikbaar zijn. Maar er moet wel duidelijk een afweging worden gemaakt en er dient onderbouwd te worden welke risico's genomen gaan worden om kosten te besparen.

5.3.4 Stap 4: analyse van verschillen tussen gewenste en beschikbare middelen (gap-analyse)

In het geval van een nieuwe situatie is men snel klaar met stap 4. Er is nog niets, dus moet alles nog geïmplementeerd worden om de gewenste situatie te bereiken. Dit is lang niet altijd het geval en dan is het raadzaam om de huidige situatie te vergelijken met de gewenste situatie. Een gap-analyse laat zien wat al voldoet aan de gewenste situatie, waar aanpassingen nodig zijn en met welke investeringen (materieel en mensen) tot de gewenste situatie kan worden gekomen.

5.3.5 Stap 5: implementatie

Stap 5 wordt uitgebreid beschreven in hoofdstuk 6.

5.3.6 Stap 6: evaluatie

De evaluatie van het ontwerp is essentieel voor het functioneren van de omgeving en voor de betrouwbaarheid. Zonder een goede evaluatie is het niet mogelijk om te zien of het eisenpakket goed ingevuld is en of het eisenpakket (nog) juist is. Het kan overigens belangrijk zijn om het ontwerp te laten toetsen voortdat tot de implementatie van de ontworpen firewall wordt overgegaan.

5.4 Bijzondere domeinsituaties

In paragraaf 5.3 is er op basis van standaardsituaties, waarin verschillende domeinen in relatie tot elkaar voorkomen, een koppelingenmatrix gepresenteerd. Deze matrix beperkt zich tot de standaardsituaties waarin twee domeinen zich ten opzichte van elkaar kunnen bevinden. Maar door de technische ontwikkelingen van de afgelopen jaren komen we tegenwoordig ook andere situaties tegen. Aan de hand van een aantal veelvoorkomende situaties bespreken we enkele bijzonderheden en de bijbehorende maatregelen. Het spreekt voor zich dat het overzicht niet

uitputtend is, we geven slechts aan hoe met dergelijke afwijkingen omgegaan kan worden. Zie figuur 5.6.

Maatregelen / Aard verbinding	Pakket-inspectie	Applicatie-inspectie		Intrusion detection	Encryptie	DMZ
		Proxy	Content screening		VPN	
Een (of enkele) webserver(s)	✓			✓		✓
Webapplicaties	✓	✓	✓	✓		✓
Internet access only	✓	✓	✓			
Draadloos netwerksegment	✓	✓		✓	✓	
Applicatieservers	✓					✓
Laptops	✓			✓	✓	
Domeinscheiding ontwikkel-productie		✓	✓	✓		

Figuur 5.6 Matrix bijzondere domeinsituaties

Toelichting matrix bijzondere domeinsituaties

Eén (of enkele) webservers vormt (of vormen) het te beschermen domein

Als het te beschermen domein erg klein is, is het zeer aannemelijk dat de maatregelen minder drastisch zijn dan men gezien het verschil tussen de domeinen zou verwachten. Dit is natuurlijk zeer afhankelijk van de dataclassificatie en de risicoanalyse.

Webapplicaties

Bij een webapplicatie is het wenselijk om de applicatie in meerdere domeinen op te delen. De verschillende delen van de applicatie hebben verschillende behoeftes op het gebied van beveiliging. De presentatiekant van de applicatie is een omgeving waarin uitsluitend leesacties worden uitgevoerd. Deze kan met een beperkte bescherming aan internet worden gekoppeld. Het applicatiegedeelte waar de verwerking plaatsvindt, zal beter moeten worden beschermd. Hiertoe worden drie domeinen onderscheiden: het onveilige internet, de presentatielaag en de applicatielaag, waarbij de applicatielaag uitsluitend via de presentatielaag benaderd mag en kan worden.

Internet access only

Een veelvoorkomende situatie is de koppeling van een vertrouwd aan een onvertrouwd domein, waartussen asynchrone communicatie plaatsvindt. Een voorbeeld hiervan is de aansluiting van een kantooromgeving op internet. Hierbij is het uitsluitend de bedoeling dat de gebruikers van de kantooromgeving informatie kunnen ophalen vanaf internet. De omgeving bevat geen diensten voor internetgebruikers. In dit geval is er uitsluitend behoefte aan de firewall-functionaliteit die het mogelijk maakt om veilig en gecontroleerd internet op te gaan.

Draadloos netwerksegment

Een draadloos netwerk dat gebruikt wordt binnen een organisatie, moet gezien de aard van een dergelijk netwerk – het is draadloos en de signalen kunnen tot ver buiten het pand ontvangen worden – per definitie als onbekend en dus onvertrouwd behandeld worden. Bij draadloos verkeer is goede authenticatie en encryptie een noodzaak.

Applicatieservers

Binnen een organisatie kan men ervoor kiezen om één of meer applicatieservers op basis van de data en de handelingen die daarmee uitgevoerd worden, in een specifiek domein te plaatsen. In de regel wordt een applicatieserver geplaatst, omdat een deel van de gebruikers niet 100 procent vertrouwd kan worden. Het is niet altijd mogelijk om de gebruikers van een domein ook binnen het domein te brengen. In dit geval zijn de applicatieservers onderdeel van het eigen en dus vertrouwde domein en zouden de gebruikers tot het deels vertrouwde domein kunnen worden gerekend.

Laptops

Laptops worden niet alleen binnen de eigen omgeving gebruikt, het komt bijvoorbeeld vaak voor dat iemand in zijn eigen huis met een laptop op het bedrijfsnetwerk mag werken. Dit betekent dat de laptop (op zichzelf te beschouwen als een deels vertrouwd domein) zich bevindt in een onbekend domein. Er dienen dus maatregelen te worden genomen om de laptop te beschermen tegen het onbekende domein waarin hij zich bevindt. Maar ook de communicatie met het eigen domein moet worden beschermd. Dit gebeurt bij voorkeur met behulp van encryptie.

In feite moet de laptop gezien worden als een geheel zelfstandig domein. Dit betekent dat bij het opstellen van een beveiligingsplan voor laptops ook voldaan moet worden aan de eisen die opgelegd worden aan een domein zoals beschreven in paragraaf 5.3. Een laptop die zich in een onveilige omgeving bevindt en die contact maakt met het bedrijfsnetwerk, zal dus moeten worden voorzien van filters, proxy's, intrusion detection, et cetera. Ook zal gegarandeerd moeten worden dat al deze zaken naar behoren functioneren, daarom is het meer dan wenselijk om deze middelen vanaf een centrale locatie aan te sturen.

Domeinscheiding: ontwikkel- en productieomgeving

Het hanteren van de term 'domein' is in dit verband wellicht verwarrend, maar deze situatie komt regelmatig voor. Er is sprake van een domeinscheiding als binnen een groter bedrijfsnetwerk een ontwikkel- en een productieomgeving kunnen worden onderkend, die van elkaar gescheiden moeten worden. Dat is onder andere noodzakelijk op grond van dataclassificatie of externe regelgeving. Als het fysiek scheiden van de netwerken van beide omgevingen niet mogelijk is, dan kan een firewall een oplossing zijn.

5.5 De-militarized zone

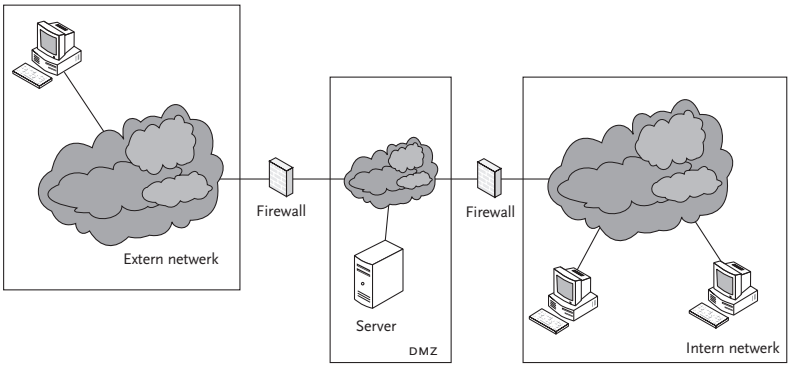
De zogenaamde *de-militarized zone* (DMZ) is geen onderdeel van de firewall. DMZ is een netwerkelement dat binnen de firewall-topologie vaak wordt ingezet, maar op zichzelf geen filterende werking heeft. Het is echter een dermate belangrijk ontwerpprincipe dat we er in deze studie wel dieper op ingaan.

Het ontwerpprincipe waarop de DMZ is gebaseerd, is compartimentalisatie. Door dit principe te hanteren, kan worden voorkomen dat compromittering van één onderdeel van het netwerk zich zal verspreiden naar andere onderdelen. De DMZ is de meest voorkomende vorm van compartimentalisatie. De kreet 'DMZ' komt uit de krijgskunde en is de bufferzonde tussen twee vijandige strijdmachten. In de netwerkwereld wordt DMZ gebruikt als ontkoppelpunt voor verkeer tussen een vertrouwd en een minder vertrouwd netwerk.

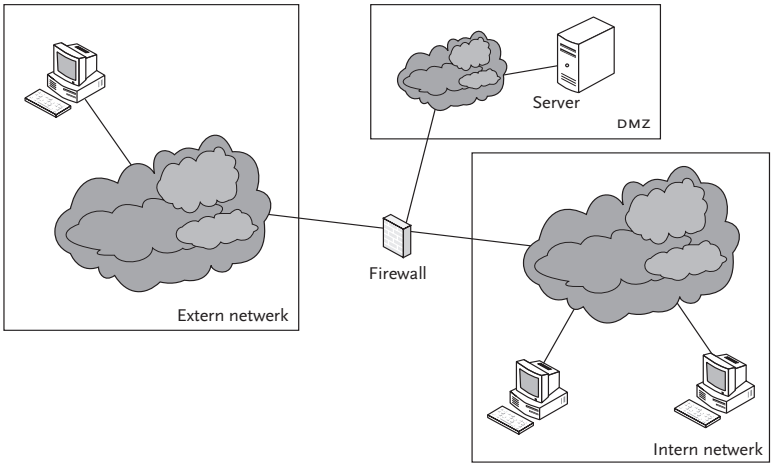
Een DMZ biedt een bedrijf de mogelijkheid om gecontroleerd aan derden te gekoppeld te zijn en informatie uit te wisselen. Maar ook binnen een bedrijf kunnen verschillende domeinen gedefinieerd worden. Zo is de HRM-afdeling in de praktijk vaak afgeschermd van de overige bedrijfsonderdelen vanwege de gevoeligheid en vertrouwelijkheid van HRM-gerelateerde informatie.

Wij onderscheiden de volgende typen DMZ:
- dubbele firewall;
- *poor mans* DMZ;
- dual homed hosts.

Figuur 5.7, 5.8 en 5.9 geven enkele verschillende typen DMZ grafisch weer.
In figuur 5.7 worden er slechts twee communicatiestromen toegestaan, een tussen het externe netwerk en de server in de DMZ en een tussen het interne netwerk en de server in de DMZ. Het is een goede gewoonte om bij deze architectuur twee verschillende soorten en/of merken firewalls te gebruiken. Op die manier kan worden voorkomen dat een zwakke plek in een van de firewalls toegang tot de te beschermen omgeving verschaft.



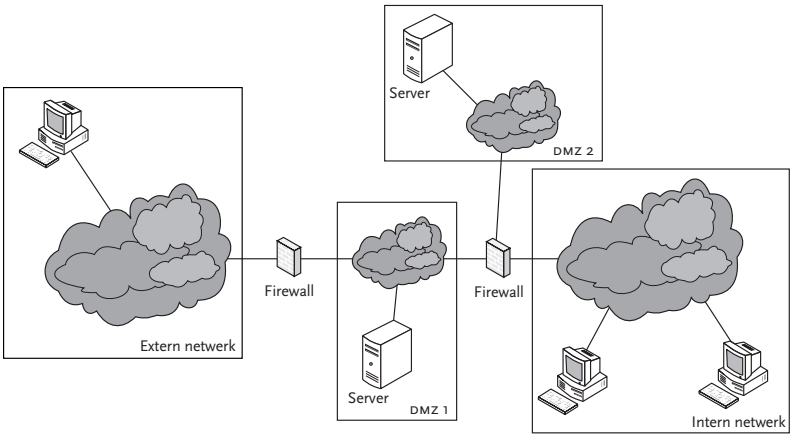
Figuur 5.7 Dubbele firewall



Figuur 5.8 Poor mans DMZ

Ook in figuur 5.8 worden er slechts twee communicatiestromen toegestaan, een tussen het externe netwerk en de server in de DMZ en een tussen het interne netwerk en de server in de DMZ.

Er zijn in de praktijk veel combinaties mogelijk van de verschillende DMZ-vormen. Vaak kiest men dan ook voor een hybride vorm, zie figuur 5.9.



Figuur 5.9 Hybride vorm

Doordat het netwerkverkeer in een DMZ 'ontkoppeld' kan worden, is het mogelijk om cryptografie en filtering, twee beveiligingsmechanismen die haaks op elkaar staan, te koppelen. Verkeer over een onvertrouwd netwerk wordt versleuteld verstuurd naar een DMZ, alwaar de informatie wordt gedecodeerd. Hierna kan het verkeer geïnspecteerd en vervolgens doorgestuurd worden.

DMZ's worden ook vaak gebruikt om koppelingen met gelieerde organisaties op een beveiligde manier tot stand te brengen. Via een DMZ kunnen op een gecontroleerde wijze gegevens worden uitgewisseld met een derde partij, zonder dat er volledige toegang tot het interne domein verleend hoeft te worden. Zo'n constructie wordt ook wel 'extranet' genoemd.

Er zijn vele manieren om een DMZ in te richten. De gouden regel is dat de elementen in een DMZ géén data behoren te bevatten. De DMZ dient enkel voor translaties, proxy's en inspectie.

Een bijzondere toepassing van het DMZ-ontwerpprincipe is de realisatie van de veilige infrastructuur *domain name system* (DNS). De belangrijkste netwerkactiviteiten met betrekking tot DNS is het vertalen van namen naar IP-adressen (en andersom) en het uitwisselen van zone-datafiles. Er zijn al veel gevallen bekend waarin het openstellen van DNS-poorten in firewalls is misbruikt voor netwerkaanvallen, die variëren van het opzetten van UDP-tunnels, tot aanvallen op de DNS-infrastructuur zelf.[1]

5.6 Firewall als onderdeel van het beveiligingsbeleid

Hoewel er in dit hoofdstuk richtlijnen worden gegeven voor het opstellen van een firewall-ontwerp, is het natuurlijk niet zo dat er sprake is van een onafhankelijk element binnen de totale infrastructuur. Het is belangrijk dat de ontworpen oplossing goed aansluit bij de organisatie die beschermd dient te worden. Het is zelfs goed mogelijk dat een 'minder veilig' ontwerp beter bij de organisatie aansluit en daardoor uiteindelijk betere resultaten geeft.

De algemene bedrijfsprincipes, en de beveiligingsprincipes in het bijzonder, zijn leidend bij het nemen van beslissingen in elke fase van het ontwikkelproces. Ze geven de kern aan waaraan elke oplossing zo veel mogelijk moet voldoen. Daar waar principes tegenstrijdig zijn, geeft de onderlinge weging de relatieve zwaarte van elk principe aan. Er moet bovendien niet geschroomd worden om te constateren dat het binnen de geldende regels misschien niet mogelijk is om tot een ontwerp te komen. In dat geval is het de verantwoordelijkheid van de organisatie om te kiezen: stoppen met het project, of wijzigingen aanbrengen in de principes en daarbij akkoord gaan met de risico's.

5.7 Voorbeeld

In deze paragraaf wordt met een voorbeeld gedemonstreerd hoe aan de hand van de in paragraaf 5.3 beschreven methode een firewall voor een webwinkel kan worden ontworpen. Aangezien de stappen 4 tot en met 6 niet in dit voorbeeld uit te werken zijn, blijft het voorbeeld beperkt tot de eerste drie stappen van de methode.

5.7.1 Stap 1: analyse en eisen

We willen een internetwinkel oprichten, een webwinkel. De volgende eisen worden gesteld aan de webwinkel:

- de webwinkel moet zeven dagen per week 24 uur beschikbaar zijn, de *back office* uitsluitend gedurende kantooruren;
- de webwinkel en back office moeten beveiligd zijn tegen de boze buitenwereld;
- de webwinkel moet zeer zorgvuldig omspringen met financiële informatie van klanten;
- de webwinkel moet zeer zorgvuldig omspringen met klantgegevens, de klantgegevens moeten, naast het interne bedrijfsproces, uitsluitend voor de klant in kwestie toegankelijk zijn;
- communicatie van de webwinkel naar back office verloopt via een veilige, specifieke en bedrijfseigen infrastructuur, niet in handen van of te benaderen door derden;

– de webwinkel moet voor alle bezoekers een beschikbaarheid hebben van minimaal 99,5 procent gedurende 7 keer 24 uur;
– de webwinkel moet minimaal vijfhonderd bezoekende internetklanten per uur tegelijk kunnen bedienen;
– de webwinkel moet minimaal 7 keer 20 uur de mogelijkheid bieden orders te plaatsen en daarbij minimaal tien orders per minuut kunnen afhandelen.

Op basis van de bovenstaande eisen en wensen kunnen we nu de analyse maken.

Inventarisatie van de domeinen

In het geval van deze webwinkel is er sprake van minimaal drie domeinen:
1 het internet;
2 de *front-end* van de webwinkel;
3 de *back-end* van de webwinkel.

Tijdens het ontwerpproces kunnen er nog meer domeinen ontstaan, zoals dat van de leverancier of een DMZ.

Dataclassificatie

Er worden in deze omgeving drie typen data onderscheiden: de productinformatie, de klantinformatie en de financiële informatie. Om verschillende redenen zullen deze beide laatste soorten niet publiekelijk beschikbaar mogen zijn, of worden gewijzigd. Naast deze gevoelige informatie bevat de webwinkel ook minder gevoelige informatie: de presentatie van de webwinkel, bijvoorbeeld in de vorm van plaatjes van producten die verkocht worden.

Risicoanalyse

Het opstellen van de risicoanalyse is een apart proces dat we hier niet zullen nalopen, we beperken ons tot de conclusie dat de webwinkel goed beschermd moet worden, omdat er serieuze financiële en juridische risico's kunnen ontstaan als onbevoegden bij de informatie kunnen komen. Ook zal ervoor moeten worden gezorgd dat de webwinkel goed beschikbaar blijft. Als de webwinkel niet beschikbaar is, zullen er ook geen inkomsten kunnen worden gegenereerd. Op basis van de vertrouwensmatrix

classificeren we internet hier als een onvertrouwd domein. De front-end is een deels vertrouwd domein en de back-end een vertrouwd domein.

5.7.2 Stap 2: logisch ontwerp

Bij het opstellen van het logisch ontwerp bepalen we hoe de datastromen lopen en welke filterende maatregelen we moeten toepassen.

Datastromen

In het voorbeeld van de webwinkel zijn er drie hoofdstromen te onderscheiden:

- De internetgebruiker communiceert met de front-endservers. Het zal voor hem niet relevant zijn wat er achter deze servers gebeurt.
- De front-endserver haalt de informatie die hij niet heeft van de back-endserver. Hier zullen de transacties worden afgehandeld.
- De back-endserver zal de transacties afhandelen met het logistieke en het financiële systeem.

In dit ontwerp beperken we ons tot de 'voorkant' van de omgeving. We zien hier twee overgangen. Dit komt overeen met de drie domeinen.

Selectie van de filterende maatregelen

De webapplicatie is een bijzondere domeinsituatie, zoals blijkt uit figuur 5.10.

Maatregelen / Te beveiligen componenten	Pakket-inspectie	Applicatie-inspectie		Intrusion detection	Encryptie	DMZ
		Proxy	Content screening		VPN	
Webapplicaties	✓	✓	✓	✓		✓

Figuur 5.10 Matrix bijzondere domeinsituaties

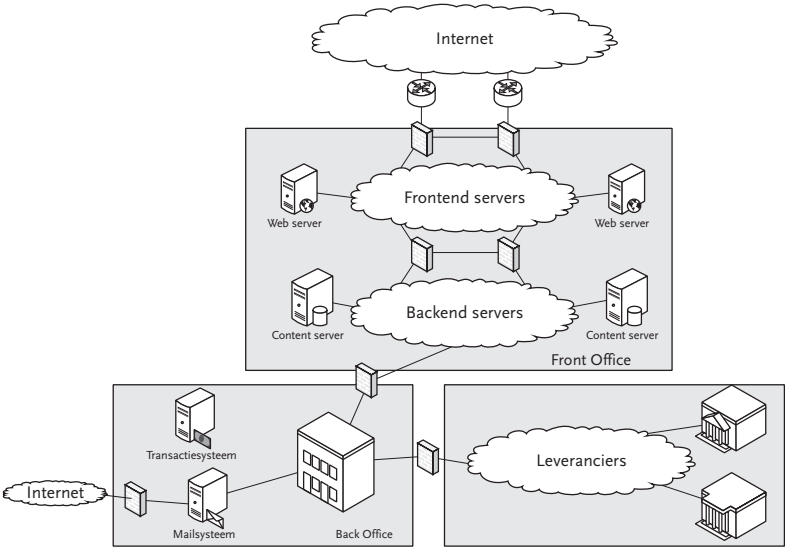
Er zijn in dit voorbeeld drie domeinen, deze plaatsen we achter elkaar waardoor we twee beveiligingslagen moeten invullen. Welke functionaliteit plaatsen we waar?

Buitenste beveiligingslaag:
– netwerkfilter;
– proxy/contentscanning;
– intrusion detection.

Binnenste beveiligingslaag:
– netwerkfilter.

De front-endservers worden geplaatst in een DMZ, deze servers bevatten geen data en voorzien uitsluitend in de grafische presentatie en plaatsen de verzoeken bij de back-endserver. Verder plaatsen we op alle servers intrusion-detectionsoftware.

Een logisch ontwerp kan er dan uitzien zoals in figuur 5.11 is weergegeven.



Figuur 5.11 De logische webwinkel

5.7.3 Stap 3: functioneel ontwerp

De stappen binnen het functioneel ontwerp kunnen zeer situatiespecifiek zijn. We zullen ze hier niet uitwerken, maar we zullen wel een voorbeeld geven van de eisen die aan deze omgeving gesteld kunnen worden:

- De orderbevestiging loopt via e-mail terug naar de klant, gebruikmakend van een aparte e-mailserver ten behoeve van orderbevestiging. Deze mailserver is via de eigen firewall-functionaliteit (met uitsluitend de betreffende poorten geopend) gekoppeld aan internet. De server heeft geen directe koppeling met de servers van de webwinkel, hij is in het back-officedomein geplaatst.
- De firewall-configuratie tussen *front office* en internet moet een beschikbaarheid hebben van minimaal 99,5 procent gedurende 7 keer 24 uur (de openingstijden van de webwinkel) en moet daarom redundant zijn.
- De firewall tussen front en back office moet een beschikbaarheid hebben van minimaal 99,5 procent gedurende 7 keer 20 uur.
- De verwerkingscapaciteit van de firewall moet snel uit te breiden zijn waarbij de webwinkel zo kort mogelijk (< 30 minuten) onbereikbaar is voor bezoekers.

Op basis van het logisch ontwerp en de overige eisen kunnen we overgaan tot het beschrijven van de fysieke elementen, software en hardware selecteren en de beheersmaatregelen bepalen.

Noten

1 Er kunnen diverse maatregelen worden getroffen om DNS op een veilige manier toe te passen. Zorg bijvoorbeeld dat zonedata-uitwisseling alleen is toegestaan voor geautoriseerde DNS-servers en pas bij voorkeur 'split-DNS-infrastructuur' toe, waardoor een gescheiden interne en externe DNS-omgeving ontstaat. De externe omgeving bevat alleen gegevens die van belang zijn voor connectiviteit vanaf internet, en geen gegevens die nodig zijn voor het functioneren van het interne netwerk. Daarvoor wordt de interne DNS-omgeving gebruikt. Op deze manier kan op de firewall een veel gerichtere DNS-policy worden opgesteld.

6 Implementatie

Aan de hand van het ontwerp wordt een blauwdruk gemaakt, op basis waarvan de daadwerkelijke inrichting van de firewall-omgeving wordt opgebouwd. Afhankelijk van het detailniveau dat uit de ontwerpcriteria wordt afgeleid, zullen er nog keuzes gemaakt moeten worden over onder andere de toe te passen producten en het netwerkontwerp.

Het is van belang om tijdens de implementatiefase zowel de security policy als de beheeractiviteiten in het oog te houden, om te waarborgen dat de firewall datgene doet waarvoor hij is aangeschaft en dat de beheeractiviteiten hierop kunnen worden afgestemd. Omgekeerd dient bij de implementatie rekening gehouden te worden met de toekomstige beheeractiviteiten. Beide kunnen gerealiseerd worden door tijdens de implementatiefase contact te houden met de *security officer* en de beheerpartij.

Om een goede implementatie van een firewall-omgeving te verkrijgen, is een stappenplan onontbeerlijk. Een dergelijk stappenplan kan er als volgt uitzien:

- opstellen technisch ontwerp van het firewall-systeem;
- aanschaffen van de benodigde componenten/software/documentatie;
- installeren hardware/software en *hardening*;
- tunen filtermechanismen;
- inrichten logging en alerting;
- testen;
- exploiteren.

6.1 Technisch ontwerp van het firewall-systeem

In het voorgaande hoofdstuk staan de ontwerpcriteria van de firewall beschreven. Op basis van een analyse van de gewenste functionaliteit, die vanuit de bedrijfsprocessen van een filterende koppeling wordt verlangd (zie hoofdstuk 5), en van de bedreigingen waartegen firewall-functies (zie hoofdstuk 4) moeten worden ingezet, wordt het technische ontwerp van de firewall opgesteld. Daartoe wordt een detailtekening gemaakt waarin de verschillende componenten onderscheiden kunnen worden.

In hoofdstuk 4 werden ook twee discussiepunten aangedragen: hoe moeten we omgaan met begrippen als 'binnen'/'buiten' en 'in'/'uit' en hoe met het vaststellen van de beveiligingsniveaus van de domeinen die door de koppelvlakken worden begrensd? Zo zal het 'buitennetwerk' vaak een lager beveiligingsniveau hebben dan het 'binnennetwerk'.

Deze twee discussiepunten moeten ook aan de orde komen bij elk ontwerp en iedere realisatie van een firewall. Het resultaat van deze exercitie is een autorisatiematrix, waarin wordt aangegeven welke verkeersstromen zijn toegestaan (en welke niet!) bij overgang van het ene domein naar het andere. Als er daarnaast ook wordt gespecificeerd wat voor type inhoud wordt toegestaan in deze verkeersstromen spreken we over een 'communicatiematrix'.

In het ontwerpstadium moeten de productkeuzes bekend zijn of worden. Op basis van het ontwerp kan een bestellijst worden samengesteld. Deze stap zal vaak een iteratief proces zijn waarbij de verschillende personen die de inrichting voor hun rekening nemen, betrokken zijn. Tijdens deze iteratie zal telkens weer de controleslag gemaakt moeten worden of het ontwerp nog past binnen de ontwerpcriteria en de security policy. De onderstaande ontwerpaspecten zullen in het ontwerp moeten worden uitgelicht.

6.1.1 Voorbereiding beheer

Een firewall kan alleen 'veilig' zijn wanneer deze op een consequente wijze wordt beheerd. Dat houdt in dat bij de inrichting niet alleen naar

de opbouw van de apparatuur op het moment van implementatie moet worden gekeken, maar dat ook rekening moet worden gehouden met het ondersteunende operationele beheerproces.

Niet iedere organisatie heeft de behoefte, de expertise of de capaciteit om het beheer van een firewall-omgeving zelf uit te voeren. Firewall-beheer impliceert in de regel immers 7 keer 24 uur beschikbaarheid van de achterliggende dienst en dat betekent dat ook 7 keer 24 uur ter zake deskundig beheer noodzakelijk is. Dat is voor veel organisaties niet op te brengen. In dergelijke gevallen is het een optie om deze activiteiten geheel of gedeeltelijk uit te besteden of te *outsourcen*. Sommige leveranciers leveren specifieke diensten met betrekking tot beveiliging (*managed security services*, of MMS). MMS-dienstverleners danken hun kennis en ervaring aan de verschillende soorten klanten voor wie zij werken. Dit brede blikveld biedt vooral efficiency-voordelen voor de klant.

Voor het netwerkontwerp moet de mogelijkheid bestaan dat een derde partij toegang heeft tot de firewall-componenten, zonder dat daarmee de beveiliging gecompromitteerd wordt. Door een modulair ontwerp van de omgeving en door toepassing van de principes *segregation of duties* en *least privilege* kan de mogelijkheid worden ingebouwd om deze derde partij toegang te verlenen tot de te beheren componenten.

6.1.2 Centraal versus decentraal en gedistribueerd

Afhankelijk van de behoefte en werkwijze van de organisatie, zal er in de ontwerpcriteria gekozen zijn voor het concentreren van alle onvertrouwde koppelingen op één beveiligd knooppunt, het decentraliseren van deze koppelingen op verschillende knooppunten of een mengvorm daartussen. Vaak is deze keuze afhankelijk van de fysieke locaties en van de aanwezigheid van koppelingen naar derden. De keuze heeft verschillende consequenties.

Bij een centraal koppelpunt is het veelal gemakkelijker een uniform beleid te handhaven, en is het voor een IT-manager overzichtelijker hoe en waar de informatiestromen gecontroleerd worden. Door samenvoe-

gen van informatiestromen kunnen ook kostenbesparingen gerealiseerd worden. Centrale koppelpunten hebben echter ook het nadeel dat de complexiteit juist weer toeneemt, door het grote aantal verkeersstromen dat hier bij elkaar komt. Dit kan fouten in de hand werken en vormt daardoor een groot risico ten aanzien van de beveiliging.

Met decentralisatie van koppelvlakken worden de informatiestromen echter weer duidelijker van elkaar gescheiden, wat de overzichtelijkheid en beheersbaarheid van deze informatiestromen weer ten goede kan komen. Decentrale koppelvlakken vergen echter vaak meer inspanning om het beveiligingsbeleid eenduidig te houden. Diverse (commerciële) producten bieden technische mogelijkheden om toch vanuit een centraal punt het beheer te kunnen uitvoeren en het overzicht te bewaren.

Een andere vorm van decentralisatie van de firewall-functie is het gebruik van een personal firewall op laptops die zowel binnen het eigen netwerk worden gebruikt als via internet toegang kunnen krijgen tot de informatiesystemen van de organisatie. Daarmee ontstaat een gedistribueerd beveiligingsmodel, waarbij de eindpunten over verschillende security policies moeten kunnen beschikken: een vrije policy wanneer de laptop aan het eigen netwerk is gekoppeld en een stringente policy die van toepassing is als de laptop aan een onvertrouwd netwerk wordt gekoppeld (bijvoorbeeld een privé-thuisnetwerk of internet). In deze topologie zal gestreefd moeten worden naar een centraal beheerbare personal firewall.

6.1.3 Redundantie en load balancing

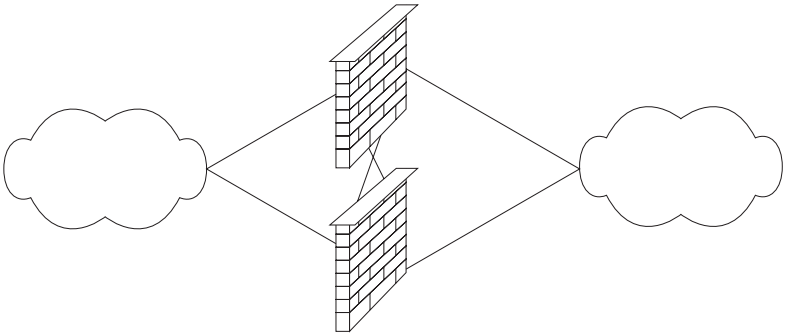
Omdat een firewall een centrale rol speelt in de beveiliging van informatiestromen naar en door het netwerk van een organisatie, wordt deze meestal als *choke-point* van de meest kritieke informatiestromen ingezet. Hiermee wordt de firewall zelf een *single point of failure*. Het falen van de firewall legt juist dan de kritieke informatiestromen stil. Ook een excessieve belasting van de firewall door een van de informatiestromen kan nadelige gevolgen hebben voor de performance van de andere stromen.

Door redundantie in te bouwen op verschillende niveaus kan een groot deel van de beschikbaarheidrisico's worden afgedekt. Denk hierbij aan het dubbel uitvoeren van netwerkkaarten en switches, dubbele *power supplies*, een RAID-configuratie of zelfs aan het dubbel uitvoeren van de gehele firewall. In dat laatste geval zal er vaak additionele software of configuratie nodig zijn om, bij het falen van een van beide firewalls, naadloos over te kunnen gaan op de backup-firewall.

Deze redundantie impliceert een hoeveelheid niet-gebruikte capaciteit waar wel kosten voor worden gemaakt. Veel firewall-producten bieden de mogelijkheid om deze overcapaciteit alsnog te gebruiken ten behoeve van betere prestaties. Dit heeft wel tot gevolg dat de prestaties zullen verslechteren als een firewall-component faalt. In het ontwerp zal dus rekening moeten worden gehouden met de minimaal benodigde capaciteit voor iedere informatiestroom, zodanig dat deze ook nog geleverd kan worden als niet de volledige capaciteit beschikbaar is.

Een voorbeeld van hoge beschikbaarheid

In deze paragraaf is het accent gelegd op het feit dat de verbinding tussen de twee domeinen een zeer hoge beschikbaarheid moet hebben. Dit resulteert in het dubbel uitvoeren van de aansluitingen en het dubbel uitvoeren van de firewalls zelf.



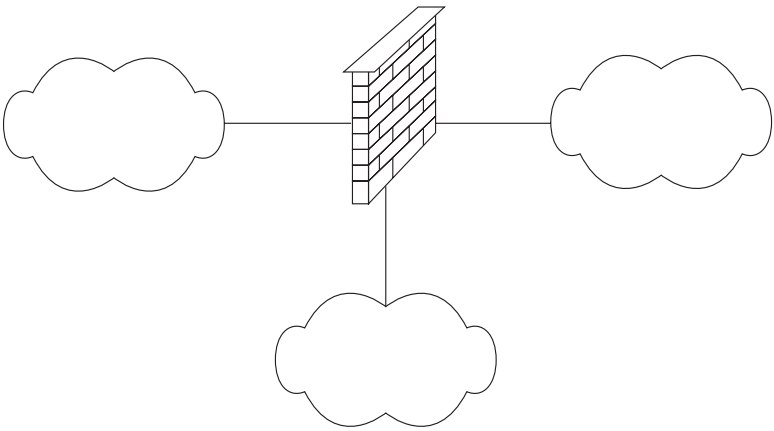
Figuur 6.1 Verschijningsvorm firewall met hoge beschikbaarheid

In de in figuur 6.1 geschetste situatie zal bij het falen van maximaal één verbinding per domein en maximaal één firewall toch verbinding mogelijk zijn tussen de twee domeinen. Wat deze domeinen voorstellen is hier niet van belang.

Aangezien het relatief lastig is om een zogenaamd *statefull failover*-systeem te maken (een systeem waarbij alle contextuele gegevens correct worden doorgegeven aan de verbinding die actief wordt), wordt vaak een *stateless*-methode gebruikt. Dat houdt in dat in de functionaliteit vaak alleen een statisch pakketfilter wordt gebruikt. Indien ook contextuele informatie meegenomen moet worden, kan men een ander type filter kiezen. Dit gaat wel ten koste van administratie- en interpretatie-overhead, zodat er vaak een krachtige machine met snelle algoritmen gebruikt moet worden.

Een voorbeeld van een koppeling van meerdere domeinen

Het voorbeeld in figuur 6.1 gaat over het koppelen van twee domeinen. In de praktijk is er vaak sprake van een samenspel van meer dan twee domeinen, waarbij er verschillende manieren van reguleren tussen deze domeinen nodig zijn.



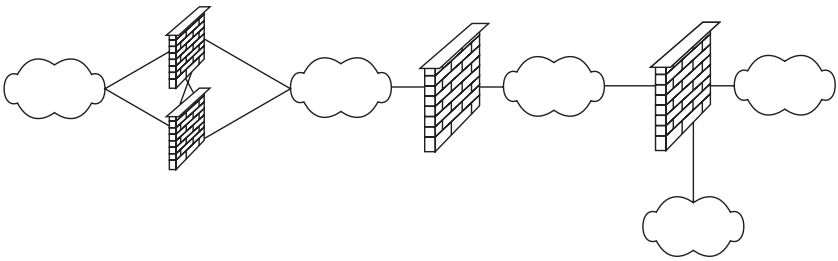
Figuur 6.2 Verschijningsvorm firewall met koppeling van meerdere domeinen

Figuur 6.2 kan bijvoorbeeld de realisatie zijn van een situatie waarbij twee domeinen informatie moeten kunnen uitwisselen en daarvoor een derde domein creëren, waartoe beide domeinen toegang hebben zonder dat de domeinen rechtstreeks toegang tot elkaar hebben. Een concrete invulling is bijvoorbeeld een koppeling naar het bedrijfsnetwerk (domein 1) en een koppeling naar internet (domein 2), zodat partners via internet naar de servers in de DMZ (domein 3) kunnen.

Bij meerdere domeinen kunnen er ook meerdere typen firewalls gekozen worden. In bovenstaand figuur is dat niet logisch, maar wel mogelijk. Afhankelijk van de wensen zoals die in de ontwerpcriteria zijn verwoord, zal er waarschijnlijk één type firewall worden gekozen, die minimaal aan deze ontwerpcriteria voldoet.

Een samengesteld voorbeeld

Uiteraard is de praktijk vaak complexer dan hierboven beschreven. Het voorbeeld in figuur 6.3 probeert de complexiteit weer te geven. Dit voorbeeld is gebaseerd op zowel een koppeling met hoge beschikbaarheid, waarbij het linkerdomein toegang krijgt tot het domein dat tweede van links staat aangegeven, als op de situatie waarin er nog drie andere domeinen zijn, waarvoor aparte regulering plaatsvindt.



Figuur 6.3 Verschijningsvorm firewall samengesteld

Een praktijkvoorbeeld: het linkergedeelte stelt de toegang via internet naar een aantal e-commerceservers voor, gevolgd door beveiligde koppelingen naar zowel de back-endsystemen van die website als naar de systemen van de leverancier(s).

In dit samengestelde voorbeeld is het mogelijk om tussen de verschillende domeinen afhankelijk van de ontwerpcriteria diverse typen firewalls te implementeren. Zo kan het type firewall dat de internetkoppeling realiseert een zwaarder type firewall zijn dan de firewall die de verschillende domeinen in de back-end van elkaar scheidt.

6.1.4 Out-of-bandmanagement

Het scheiden van netwerkverkeer op basis van functionaliteit is belangrijk voor het beveiligen van componenten. Vooral de scheiding van productie- en managementverkeer is belangrijk. Het is daarom aan te bevelen om het beheerverkeer (logging, alerts en configuratiewijzigingen) via een ander netwerk te laten verlopen dan het productieverkeer. De term *out-of-band* (OOB) duidt aan dat het netwerkverkeer voor productie en beheer van elkaar gescheiden is.

Out-of-bandmanagement levert waarborgen op voor de integriteit van de omgeving. Het creëren van een tweede netwerkverbinding voor alle componenten kan echter onacceptabel hoge kosten met zich meebrengen. In dat geval kan met behulp van VPN-tunnels toch een functiescheiding tussen netwerkmanagement- en productieverkeer worden aangebracht, zonder dat er een apart fysiek transportnetwerk nodig is.

Deze oplossing heeft echter wel consequenties voor het principe van scheiding van functies. Het beheren van de routeringsfunctie van het netwerk waarover VPN getransporteerd wordt, is bijvoorbeeld niet langer onafhankelijk van deze routeringsfunctie zelf.

6.2 Aanschaf

Bij de aanschaf van hardware en software dient eveneens aandacht geschonken te worden aan de benodigde onderhouds- en *upgrade*-contracten. Indien nodig zal er ook voor additionele training voor het onderhoudspersoneel gezorgd moeten worden.

6.2.1 Hardware en software

Voorafgaand aan de aanschaf van hard- en software wordt eerst een product- en leverancierskeuze gemaakt. Daartoe zal een pakket van functionele en technische eisen opgesteld worden, op basis waarvan een eerste selectie kan plaatsvinden. Het opstellen van een dergelijke selectielijst is in grotere organisaties noodzakelijk om aan te kunnen tonen dat de selectie op zakelijke gronden heeft plaatsgevonden. Enkele selectiecriteria zouden kunnen zijn: ICSA-certificering van het product (al is die tegenwoordig nauwelijks meer onderscheidend), functionele en technische schaalbaarheid en toepassing van open standaarden.

Bij de aanschaf van de hardware en software zal een betrouwbare leverancier gekozen moeten worden. Grotere organisaties hebben vaak al een *preferred supplier* met wie een goede relatie is opgebouwd. De leverancier kan ook ondersteunend zijn in de opbouw van de bestelling om te voorkomen dat kleine, maar essentiële onderdelen zoals bekabeling, inbouwkits, additioneel benodigde licenties en eventueel benodigd gereedschap niet over het hoofd gezien worden. Daarnaast verdient het aanbeveling om zo veel mogelijk aan te sluiten bij bestaande standaards. Dit levert voordelen op bij bijvoorbeeld het op voorraad hebben van reserve-onderdelen. Met het oog op de doorlooptijd moet altijd de levertijd van de hardware in het oog gehouden worden.

6.2.2 Training

De beheerders van de omgeving zullen voldoende bekend moeten zijn met de bediening van alle nieuwe componenten die in de omgeving geplaatst gaan worden. Vaak kan de leverancier van deze producten ook trainingen en certificeringtrajecten voor deze producten leveren. Het is ook mogelijk een expert in te huren die op de organisatie toegespitste trainingen kan geven. Bovendien behoort zelfstudie natuurlijk ook tot de mogelijkheden. Hiervoor moeten de middelen wel beschikbaar zijn: tijd, toegang tot documentatie en een laboratoriumomgeving waar, zonder schadelijke gevolgen, verschillende configuraties getest kunnen worden.

6.2.3 Supportcontracten

Zelfs bij de meest gerenommeerde producten zullen zich op een gegeven ogenblik storingen voordoen. Deze kunnen variëren van hardware- en softwarestoringen tot gevolgen van menselijke fouten of kwetsbaarheden in het product. Hardwarestoringen kunnen worden opgevangen door het eigen personeel, mits afdoende getraind en de benodigde reserve-onderdelen beschikbaar. Voor meer ingewikkelde storingen is het zinvol om te kunnen terugvallen op de ondersteuning van de leverancier. Deze ondersteuning kan bestaan uit het vervangen van onderdelen of gehele componenten, maar ook uit het beschikbaar stellen van updates, *bug fixes* en zelfs *on-site*-ondersteuning van ontwikkelaars in het geval van nog onbekende programmeerfouten. Supportcontracten zijn in de regel kostbaar, maar daar staat tegenover dat ze zeer waardevol kunnen zijn.

6.2.4 Testomgeving

Het beschikbaar hebben van een testomgeving bevordert de stabiliteit van de productieomgeving doordat de gevolgen van wijzigingen eerst in de testomgeving onderzocht kunnen worden. Voor een firewall-omgeving is het meestal ondoenlijk om een volledig representatieve testopstelling te realiseren, omdat alle informatiestromen volledig gereproduceerd moeten kunnen worden. Vaak wordt uit kostenoverweging gekozen voor een beperkte testopstelling waarbij alleen de informatiestroom wordt nagebootst die betrekking heeft op de voorgestelde wijziging. Voor wijzigingen met een grotere impact, zoals upgrades, moeten een uitgebreidere testopstelling en een bijbehorend testplan worden opgesteld.

6.3 Installatie hardware/software, netwerkconfiguratie en *hardening*

De installatie van hardware en software dient bij voorkeur te gebeuren zonder aangesloten te zijn op het productienetwerk, om zowel eventuele verstoringen op het productienetwerk als compromitteren van het nieuwe systeem te voorkomen. Wanneer de basisinstallatie voltooid is, kan netwerkverbinding, IP-adressering en routering geconfigureerd worden.

6.3.1 Installatie en configuratie

De meeste moderne producten zijn voorzien van uitgebreide installatie- en configuratie-instructies. Bij problemen kan men vaak terugvallen op de leverancier. Deze fase zal dan ook zelden problemen opleveren. Het is echter wel van belang dat op een gedetailleerd niveau de verschillende stappen en keuzes tijdens de installatie worden gedocumenteerd. Dit vereenvoudigt in een later stadium het zoeken naar mogelijke fouten en het reproduceren van de installatie in het geval van een *disaster recovery*.

6.3.2 Hardening

Firewall-apparatuur is meestal al ontdaan van onnodige componenten die mogelijk storingen kunnen veroorzaken of kwetsbaarheden kunnen bevatten. Veelal bestaan deze uit een 'gestripte' versie van een bestaand besturingssysteem en zijn er geen verdere acties nodig om de firewall minder kwetsbaar te maken. Bij firewall-applicaties, die op een afzonderlijk besturingssysteem geïnstalleerd worden, is het noodzakelijk om alle niet-gebruikte componenten te deactiveren of zelfs te verwijderen. Daarnaast bevatten veel besturingssystemen die *out of the box* geïnstalleerd worden, zwakke plekken in de vorm van onnodige gebruikersaccounts, slecht gekozen beveiligingsinstellingen en beveiligingslekken in essentiële onderdelen van het besturingssysteem.

Voor veel besturingssystemen zijn richtlijnen beschikbaar om ze zo veilig mogelijk maken, zonder dat de benodigde functionaliteit daardoor geschaad wordt. Vast onderdeel van deze richtlijnen is het installeren van alle beschikbare *patches* en bug fixes die door de leverancier zijn uitgebracht.

6.3.3 Beheeraccounts

Iedere wijziging op een firewall is een wijziging in de manier waarop de security policy van de organisatie wordt gehandhaafd. Het is dus belangrijk om wijzigingen te kunnen traceren, tot aan de persoon die deze

heeft doorgevoerd. Daarom moeten persoonsgebonden *user accounts* worden gebruikt. De meeste firewalls ondersteunen een dergelijke functionaliteit. Is die er niet, dan kan die via een tussenstap gerealiseerd worden. Te denken valt aan een *terminal concentrator* die, na authenticatie, toegang verleent tot de administratieve interface van de firewall.

Inherent aan beheeraccounts is het loggen van de acties die met deze accounts zijn uitgevoerd. Deze logging dient beveiligd te zijn tegen wijzigingen door degene die de acties uitvoert en er moet periodiek intern gecontroleerd worden op ongeautoriseerde wijzigingen.

6.3.4 Backup en recovery

De beschikbaarheid van de firewall is net zo cruciaal als de componenten die hij beschermen moet. Deze beschikbaarheid kan gewaarborgd worden door een redundante opstelling, maar dient in ieder geval ondersteund te zijn door een backup- en recovery-strategie.

In het geval van een firewall die op een serverplatform (bijvoorbeeld Windows, Unix of Linux) draait, zal veelal gebruik worden gemaakt van de backup-faciliteit van het betreffende besturingssysteem: hetzij een backup naar een lokaal medium (tape of cd-rom), hetzij via een centrale backup-oplossing over het netwerk naar een backup-server. Firewall-apparatuur (of *appliances*) is veelal niet in staat een backup te maken naar een lokaal medium. Hier is men aangewezen op netwerkbackup-oplossingen via FTP of TFTP.

De firewall-configuratie dient te worden beschouwd als bedrijfsgevoelige informatie en als zodanig beschermd te worden. Transport en opslag van de firewall-backup zijn kwetsbare plekken in de beveiliging van de firewall zelf. Protocollen als FTP en TFTP bieden slechts een geringe mate van beveiliging tijdens transport. Een gescheiden of een OOB-backupsegment kan een oplossing zijn.

Bij centrale backup-voorzieningen hoort het principe van wederzijdse authenticatie te worden toegepast. De firewall mag zijn backup niet versturen naar een *rogue*[1]-backupserver en een aanvraag van een roguebackupclient tot een *restore* van de firewall-configuratie mag niet gehonoreerd worden.

Een bijzonder aspect aan de recovery van een firewall is dat de firewall zelf mogelijk een ondersteunende functionaliteit biedt voor de backupvoorziening. Een probleem zou bijvoorbeeld kunnen ontstaan als een backup-server die voor correct functioneren toegang tot een DNS-server nodig heeft, maar waarbij de toegang tot deze DNS-server verloopt via dezelfde firewall die na een calamiteit hersteld moet worden.

6.4 Filtermechanismen

Op basis van de communicatiematrix kan het filtermechanisme worden geconfigureerd. Deze rulebase zal alleen dat verkeer doorlaten dat expliciet geoorloofd is, en het overige verkeer tegenhouden.

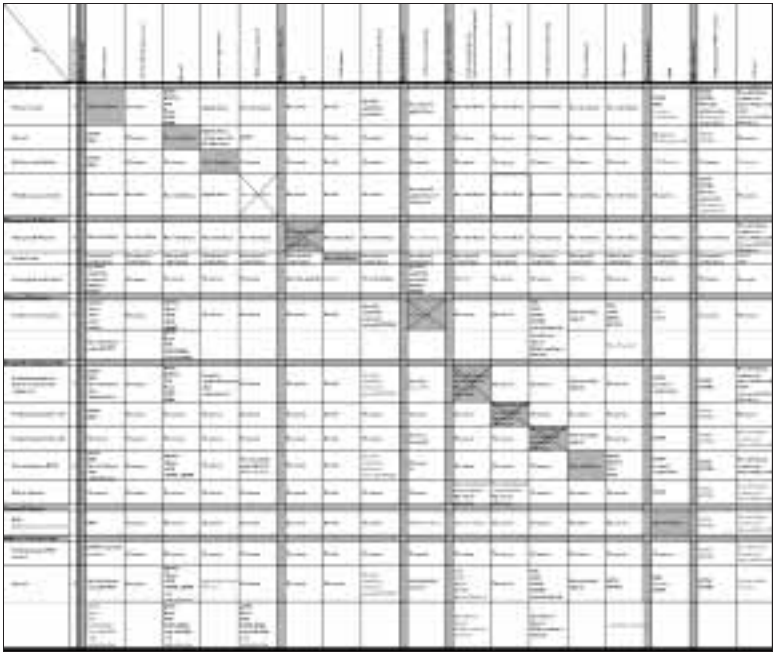
6.4.1 Communicatiematrix

Bij de implementatie van een firewall wordt de communicatiematrix vertaald naar een set van configuratieparameters. Deze set wordt ook wel de 'rulebase' genoemd. Het principe van een communicatiematrix is eenvoudig, zie figuur 6.4.

Van \ naar	Intern domein	DMZ	Extern
Intern domein	X	proxy, wet	geen verkeer
DMZ	web, mail, DNS	X	web, DNS, mail
Extern	geen verkeer		X

Figuur 6.4 Eenvoudige communicatiematrix

In grotere omgevingen kan een communicatiematrix zeer complex worden, zie figuur 6.5.



Figuur 6.5 Complexe communicatiematrix

6.4.2 Firewall rulebase, functioneel

Onafhankelijk van het gekozen firewall-product, zal de basis-rulebase min of meer op dezelfde wijze opgezet worden. In grote lijnen gaat het om de volgende regels:

1 verkeer naar firewall voor onder andere beheer van de firewall;
2 expliciete *drop and ignore rule* naar firewall;
3 expliciete *drop and log rule* naar firewall (*stealth rule*);
4 expliciete *accept rule*;
5 expliciete drop and ignore rule;
6 expliciete drop and log rule;
7 impliciete drop rule.

Via regel 1 wordt geautoriseerd verkeer, bijvoorbeeld vanaf een beheernetwerk, naar de firewall doorgelaten.

Regels 2 en 5 zijn om te voorkomen dat veelvoorkomend verkeer dat geen veiligheidsrisico vormt de logfile van de firewall vervuilt.

Regel 3 wordt ook wel de *lockdown rule* of stealth rule genoemd. Deze regel voorkomt ongeautoriseerd verkeer naar de firewall.

Hierboven is de zogenaamde *sneaky rule* niet getoond. Deze regel bepaalt dat er geen verkeer vanaf de DMZ naar het interne netwerk mag; anders zou er een risico ontstaan in het geval van een gecompromitteerde DMZ.

Bij het toepassen van het *default deny*-principe in een complexe omgeving kan een rulebase zo complex worden dat deze te onoverzichtelijk wordt om goed te kunnen beheren, of zelfs zo complex dat dit een zware performance-impact oplevert. Door toegangsregels te groeperen wordt weliswaar meer verkeer doorgelaten dan strikt noodzakelijk, maar de verkregen vereenvoudiging van de rulebase levert juist vaak een verbetering in de beveiliging op doordat de toegangscontrole inzichtelijker is.

6.4.3 Firewall rulebase, technisch

Bij het implementeren van de rulebase dient rekening gehouden te worden met de technische werkwijze van de gekozen oplossing. Op basis van welke techniek filtert het gekozen product? Is het in staat verschillende verkeersstromen te onderscheiden, wat is de efficiëntste volgorde waarin de rulebase wordt verwerkt?

Iedere configuratieparameter beschrijft een of meer netwerkconnecties met een bijbehorende actie. Zie figuur 6.6. Een netwerkconnectie wordt bepaald door de parameters:

- Source: waar komt het verkeer vandaan (wie initieert de connectie)?
- Destination: waar gaat het verkeer naartoe?
- Service: welk protocol wordt er gebruikt?

Figuur 6.6 Voorbeeld rulebase

Voor iedere netwerkconnectie kan in een regel een overeenkomstige actie bepaald worden. Voorbeelden van acties zijn:

– allow: sta het verkeer toe;
– deny: sta het verkeer niet toe;
– drop: drop het verkeer (hetzelfde als 'deny', met als verschil dat er geen verkeer naar de afzender gestuurd wordt).

Figuur 6.7 Configuratie GUI

In figuur 6.7 wordt een voorbeeld gegeven van het management van een rulebase door een programma met een *graphical user interface* (GUI).

Voorbeeld
Om http-verkeer mogelijk te maken vanaf het interne netwerk (10.1.1.0/24) naar de webserver (192.168.1.1) bevat de rulebase de volgende regel:

source	destination	service	action
10.1.1.0/24	192.168.1.1	tcp-80(HTTP)	allow

Opbouw rulebase

Bij veel firewall-producten wordt een rulebase sequentieel doorlopen totdat het verkeer voldoet aan een regel (er is een *hit*). De actie die bij de regel hoort wordt uitgevoerd, waarna de rulebase niet meer verder doorlopen wordt. Voor deze controle wordt het eerste pakketje van een netwerkconnectie gebruikt (waarbij het SYN-bit aanstaat). Zodra dit pakketje door de firewall wordt doorgelaten, wordt de connectie opgeslagen in een *state tabel*.

Dit heeft implicaties voor de opbouw van de rulebase: De regels die het meest gebruikt zullen worden, dienen in dit geval zo hoog mogelijk in de rulebase opgenomen te worden, terwijl minder gebruikte regels lager in de rulebase geplaatst kunnen worden. Er zijn ook firewalls die werken met een database-model, waarin de volgorde van de regels geen negatieve performance-impact heeft.

Impliciete regels

Naast expliciete regels bevat een firewall ook impliciete regels. Dat zijn regels uit de rulebase die niet expliciet zijn toegevoegd, maar die ontstaan door speciale instellingen binnen de firewall-configuratie. Zo staat een CheckPoint-firewall default toe dat ICMP-verkeer wordt doorgelaten. Veel firewalls hebben een impliciete drop rule: 'Verkeer dat niet voldoet aan expliciet opgegeven regels, wordt geweigerd.'

Cut through

Uit performance-overwegingen wordt in sommige firewall-implementaties gekozen voor een initieel sterke verificatie van een verbinding, waarna de verbinding als 'vertrouwd' wordt beschouwd en de mate van controle verlaagd. De Cisco PIX Firewall bevat bijvoorbeeld een zogenaamde *cut through*-proxy: bij het opzetten van de initiële connectie tussen een webclient en een webserver wordt om authenticatie gevraagd. Bij succesvolle authenticatie wordt de connectie in een state table geplaatst, waarna verdere webconnecties tussen beide adressen wordt toegestaan. Dit voorbeeld levert een risico op wanneer clients zich achter een webproxy begeven: de eerste client achter de proxy dient zich te identificeren, waarna andere clients, zonder authenticatie, 'meeliften' op de opgezette connectie.

Performance

Omdat een firewall-rulebase sequentieel doorlopen wordt, is de volgorde van rules bepalend voor zowel efficiency als security. Rules ter bevordering van de afscherming van de firewall dienen derhalve bovenaan te staan, gevolgd door de regels waarvan aangenomen kan worden dat ze vaak 'geraakt' worden. Dit is om te voorkomen dat voor ieder pakketje dat de firewall passeert de gehele rulebase moet worden afgelopen voordat er een *match* is.

6.5 Alerting, logging, monitoring en rapportage

De firewall als apparaat kan meldingen genereren in de vorm van *alerts*, logging en rapportages. Deze meldingen worden vervolgens door de beheerorganisatie afgehandeld. Bij de inrichting moet er rekening gehouden worden met deze processen: er zullen bijvoorbeeld richtlijnen moeten worden opgesteld over hoe te handelen wanneer een bepaalde melding voorkomt.

6.5.1 Alerting

Alleen die events die een zodanige impact hebben op de organisatie dat er preventieve of correctieve acties nodig zijn, moeten leiden tot alerts. Hierbij valt te denken aan gespoofte pakketten of excessief netwerkverkeer. Wijzigingen in netwerktopologie, nieuwe applicaties en zelfs een verandering in de organisatie kunnen zoveel *false positives* opleveren, dat deze alerts hun effectiviteit verliezen. Het *fine-tunen* van alerts is een continu proces. Het laten beoordelen van de log door een geautomatiseerd log-analysesysteem dat ook andere logbestanden beoordeelt, kan de effectiviteit verhogen.

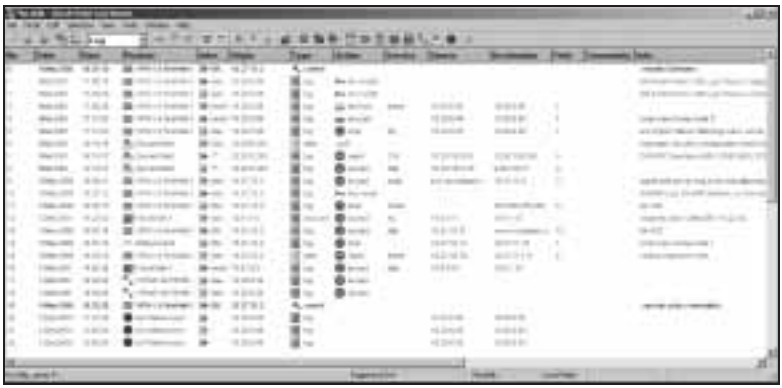
6.5.2 Logging

Een belangrijke reden om logfiles bij te houden is forensische analyse. Het is zinvol om logging te genereren van zowel geblokkeerd als doorgelaten verkeer. Ook voor logging geldt dat excessief loggen meer problemen oplevert dan oplost. *Fitness for purpose* is hierin de belangrijkste richtlijn. Bij het inrichten van logging moeten aan de volgende punten worden gedacht: benodigd detailniveau, retentieperiode, benodigde opslagcapaciteit en integriteit. Bij decentrale logging (via bijvoorbeeld het syslog-protocol of via periodieke kopieerslagen middels rsync of FTP) moeten ook de capaciteit en de integriteit van het transport onder de loep genomen worden.

6.5.3 Monitoring

Meestal wordt een firewall gezien als een middel om verkeer te blokkeren. Het belangrijkste doel van een firewall is echter het *doorlaten* van verkeer. Wanneer op de firewall een ernstige storing optreedt, kan deze geen verkeer naar de kritische netwerkonderdelen doorlaten, hetgeen een negatieve impact heeft op de beschikbaarheid van deze componenten. Monitoren van beschikbaarheid van de firewall is daarom cruciaal. Deze monitoring

dient, voordat de firewall in beheer genomen kan worden, uitgebreid getest te worden, om false positives en *false negatives* zo veel mogelijk uit te sluiten. Figuur 6.8 laat een voorbeeld zien van een monitorscherm.



Figuur 6.8 Monitoring

6.5.4 Rapportages

Het inrichten van rapportages is vaak afhankelijk van de technische mogelijkheden van de gekozen firewall-oplossing. Het doel van de rapportages moet voor ogen worden gehouden. Mogelijke doelen zijn: capaciteitsbeheer, beschikbaarheid, kostenbeheersing en incidentanalyse. De rapportage levert ook input voor een revisie van de risicoanalyse. Naast de logging die een firewall genereert over geblokkeerd verkeer, levert de informatie over de aangevraagde en doorgevoerde wijzigingen belangrijke managementinformatie op.

6.6 Testen

Na het configureren van alle parameters zal de functionaliteit van de firewall getest moeten worden. Vaak wordt hierbij alleen gelet op het doorlaten van het benodigde verkeer. Even belangrijk is echter de controle van het correct blokkeren van ongewenst verkeer, de loggingfunctie en *fail-*

over-functionaliteit. Het (laten) uitvoeren van een penetratietest vanaf het onvertrouwde netwerk, of het laten beoordelen van de rulebase voordat een belangrijke component in productie wordt genomen, zou onderdeel van het accepatieproces kunnen zijn.

Tijdens de testfase kan ook geverifieerd worden of de documentatie voldoende handvatten biedt om de gehele firewall opnieuw op te bouwen. Om zo natuurgetrouw mogelijk te testen, moet de *disaster recovery test* bij voorkeur niet worden gedaan door dezelfde personen die de inrichting en de documentatie hebben opgeleverd, maar door de personen die de test in het geval van een calamiteit ook zullen moeten doen.

6.7 Implementatie

Als laatste stap zal de firewall in de productieomgeving opgenomen moeten worden. Hierbij dienen opnieuw (acceptatie)tests uitgevoerd te worden. Met beheerders en afnemende organisatie zullen van tevoren dus afspraken gemaakt moeten worden over acceptatiecriteria. Hierbij valt te denken aan een aantal testscenario's met betrekking tot de benodigde functionaliteit (is internet toegankelijk, werkt het mailverkeer nog?) en beveiliging (worden virussen adequaat geblokkeerd, staan onnodige poorten dicht?). Afgezien van deze technische aspecten moet er tijdens de overdracht aandacht worden geschonken aan documentatie en beheerprocessen.

6.7.1 Documentatie

Tijdens de operationele fase van de firewall zal de verantwoordelijke beheerder voorbereid moeten zijn op het afhandelen van incidenten, storingen, wijzigingen, het beantwoorden van vragen en het doen van verbetervoorstellen. Het is onontbeerlijk dat hij inzicht heeft in het technisch functioneren van de verschillende componenten en het onderlinge samenspel, en dat hij de achterliggende reden van bepaalde configuratiekeuzes kent. Door nieuwe mogelijkheden in nieuwere versies van software kan het zijn dat deze keuzes achterhaald zijn.

Een ander belangrijk doel van documentatie is de reproduceerbaarheid van de inrichting en de gemaakte keuzes. Het kan bijvoorbeeld nodig zijn om, na een calamiteit, de gehele omgeving van de grond af aan opnieuw op te bouwen, maar evengoed kan een wijziging in de omgeving of in het beveiligingsbeleid het noodzakelijk maken om bepaalde keuzes bij de inrichting te herzien. De documentatie dient daarom niet enkel de configuratieparameters te bevatten, maar ook de achterliggende motivatie, de samenhang met andere parameters en componenten en de samenhang met de security policy.

6.7.2 Beheerprocessen

Tijdens de implementatie dienen de beheerprocessen te worden ingeregeld, voordat de firewall daadwerkelijk in productie gaat. In het volgende hoofdstuk worden de beheerprocessen nader uitgewerkt. Hetgeen daar wordt behandeld zal ruim van tevoren moeten worden voorbereid, zodat in de beheerfase zelf alleen sprake is van onderhoud van het beheer.

Noten

1 De term 'rogue' geeft aan dat het om een niet-geautoriseerd systeem gaat (dat zich echter wel voordoet als een legitiem systeem). Dit betekent dat er of een aanval of een poging tot misbruik van de systemen gaande is.

7 Beheer

7.1 Inleiding beheer

Een firewall is, vanwege de continu veranderende internetomgeving en de veranderende risico's, geen statisch IT-systeem. Hierdoor ligt, in tegenstelling tot de gangbare IT-systemen, extra nadruk op een *actief* beheer van de firewall, met name voor de tijdigheid van de volgende processen:

- logging en monitoring van de firewall;
- management van de doorvoercapaciteit;
- volgen van nieuwe technische mogelijkheden;
- implementatie van (tijdelijke) oplossingen (fixes en patches);
- volgen van nieuwe aanvalsmogelijkheden;
- signalering van mogelijke aanvallen;
- escalatie bij geconstateerde, al dan niet succesvolle, aanvallen en andere incidenten.

Net als voor de gangbare systemen zijn voor een firewall gedegen beheerprocessen nodig. De bekendste standaard voor de inrichting van IT-beheer is de door het CCTA, het Engelse overheidscentrum voor informatiesystemen, ontwikkelde ITIL-methodiek (*information technology infrastructure library*). Deze standaard beschrijft processen als wijzigingsbeheer, incidentbeheer, beveiligingsbeheer en hun onderlinge relaties. Het Platform Informatiebeveiliging heeft de ITIL-methodiek verder uitgewerkt in de PI-studie *Basisnormen Beveiliging en Beheer IT-infrastructuur*.

In hoofdlijnen is het beheer van een firewall vergelijkbaar met het beheer van niet-beveiligingsgerelateerde IT-systemen. Zo bestaat een firewall, net als ieder ander IT-systeem uit hardware en software, waarop

een storing kan plaatsvinden. Sommige wijzigingen kunnen via het normale beheerproces doorgevoerd worden. Voor een deel voldoet het normale beheerproces echter niet.

Omdat de firewall een mogelijke toegangspoort naar het interne netwerk is, zijn er specifieke voorwaarden waaraan het beheer moet voldoen. De urgentie van de incidenten en problemen rondom de firewall wordt bepaald door de waarde die gehecht wordt aan de vertrouwelijkheid, integriteit en beschikbaarheid van alles wat de firewall beschermt. Simpel gezegd moet er bij firewallbeheer 'korter op de bal gespeeld worden'. Meer dan bij andere IT-systemen moet het beheer gericht zijn op integriteit en vertrouwelijkheid, in plaats van op beschikbaarheid.

In dit hoofdstuk zullen wij ingaan op het beheer dat specifiek is voor een firewall. We gaan hierbij uit van standaard ITIL-processen waarbij alleen de zaken die extra aandacht vragen beschreven worden. Daarnaast behandelen we audits als belangrijk onderdeel van het beheer.

7.2 Uitgangspunten voor de inrichting van een firewall

Een firewall staat, net als alle IT-systemen, ten dienste van het bedrijfsproces. Het beheer van de firewall is dan ook geen geïsoleerd proces, het zal nauw moeten aansluiten op de afspraken die de IT-organisatie heeft gemaakt in *service level agreements* (SLA's) en op de eisen die de organisatie stelt aan de beveiliging. Deze twee zaken zijn de ingrediënten van firewall-beheer.

7.2.1 Service level management

Een SLA bevat helder meetbare en objectieve criteria voor de te leveren diensten en rapportages. Hierin zijn een aantal onderwerpen vastgelegd, die ook van belang zijn voor het beheer van de firewall:

- beschikbaarheid;
- capaciteit en transportvolume;
- beveiligingsniveau;
- openingstijden helpdesk.

Voor firewall-beheer moet een beschrijving gegeven worden van het totale service- en beveiligingsniveau: de firewall-policy. Daarin zal mede vastgelegd moeten worden wat onder een beveiligingsincident verstaan wordt en welke reactie daarop moet volgen. Bovendien zal aandacht geschonken moeten worden aan speciale bevoegdheden ten behoeve van firewall-beheer, zoals het snel mogen en kunnen ingrijpen bij beveiligingsincidenten (bijvoorbeeld het uit de lucht halen van een website).

7.2.2 Security management (beveiligingsbeleid en -beheer)

De inrichting van het beveiligingsbeheer moet een integraal deel vormen van het reguliere IT-beheer. In de PI-studie *Basisnormen Beveiliging en Beheer IT-infrastructuur* is dit ITIL-proces vanuit beveiligingsoptiek geconcretiseerd en met name ook geïntegreerd met het beveiligingsbeheer.

Het beveiligingsbeheer geeft aan welke (beveiligings)uitgangspunten, doelstellingen, principes, normen en nalevingseisen voor de organisatie van belang zijn. Hierin worden de rollen en verantwoordelijkheden vastgelegd voor de uitvoering en beheersing van informatiebeveiliging in de organisatie. Binnen de beheerprocessen worden de bevoegdheden voor het tijdelijk onderbreken van de serviceverlening beschreven, evenals voor het communiceren met de exploitatieorganisatie en de klantorganisatie en het in gang zetten van nood- of escalatieprocedures.

Onderdeel van de uitwerking van beveiligingsbeheer is het uitvoeren van een risicoanalyse voor elk proces en IT-systeem. Het resultaat is een set beveiligingsuitgangspunten waar (ook) de firewall deel van moet uitmaken. De algemene elementen die bijdragen aan het realiseren van het beheer van een firewall-oplossing, worden benoemd in het beveiligingsbeleid. De specifieke elementen die de voorwaarden voor het operationele beheer van een firewall-oplossing beschrijven, worden benoemd in de firewall-policy.

De firewall-policy omschrijft in hoofdlijnen de connecties en connectiemethoden die toegestaan zijn ('verkeersplan') en dient uiteindelijk als leidraad voor het invullen van de rulebase van de firewall. De firewall-policy bevat naast een functionele beschrijving van de instellingen ook

procedures voor aanvragen, autoriseren en uitvoeren van wijzigingen in de inrichting en instellingen van de firewall. In de praktijk zijn vier implementaties van een firewall-policy te onderscheiden. Zie tabel 7.1 voor de implementaties in volgorde van toenemend beveiligingsniveau.

Tabel 7.1 Implementatievormen firewall-policy

1	Permit any... - alles mag:	In deze policy wordt al het verkeer doorgelaten.
2	Explicit deny	Enkel specifiek verkeer wordt geblokkeerd.
3	Explicit permit	De aanbevolen implementatie van een firewall-policy. Een betere beveiliging doordat enkel specifieke connecties (http, smtp, etc) worden doorgelaten.
4	Explicit permit met content filtering	Enkel specifiek verkeer, geleid over een proxy, wordt toegestaan. Als extra toevoeging op de tweede policy kan het verkeer nu gelogd en gefilterd worden. Voor diverse protocollen bestaan verschillende proxy's. Bekende voorbeelden zijn: – smtp: inbound/outbound virusscanning – http: outbound only, virusscanning en blokkeren ongewenste sites.

7.2.3 Organisatie

De invulling van een firewall-policy vereist een multidisciplinaire aanpak met medewerking van gebruikers, managers, applicatieontwerpers, applicatie-, systeem- en netwerkbeheerders, risicomanagers en auditors. Daarnaast kan voor specialistische kennis gebruik worden gemaakt van externe beveiligingspecialisten, zodat men op de hoogte blijft van de nieuwste ontwikkelingen, trends, normen en beoordelingsmethoden.

De organisatie dient zorg te dragen voor het beschikbaar stellen van de benodigde kennis. Denk hierbij aan het binnenhalen van medewerkers met firewall-kennis, maar ook aan het beschikbaar stellen van de juiste documentatie, zoals SLA's en het beveiligingsbeleid. Daarnaast is de organisatie verantwoordelijk voor het benoemen van de verantwoordelijkheden en rechten van de medewerkers in het wijzigingsbeheer.

Belangrijk hierbij is een strikte scheiding tussen de persoon die de wijziging autoriseert (bijvoorbeeld de security officer) en de persoon die de wijziging doorvoert (bijvoorbeeld de firewall-beheerder).

Een voorbeeld van verantwoordelijkheden is opgenomen in tabel 7.2.

Tabel 7.2 Verantwoordelijkheden

Manager	– vaststellen bevoegdheden van firewall-beheerder, security officer en intern cert – uitdragen beveiligingsbewustzijn
Helpdesk/ incidentmanagement	– registreren beveiligingsincidenten – rapporteren incidenten en trends – melden beveiligingsincident aan firewall beheerder (escalatie niveau 1)
Firewall-beheerder	– operationeel en technisch beheer – contact met externe firewall-leveranciers – volgen van ontwikkelingen en vulnerabilities – voorstellen verbeteringen (upgrades, patches, bugfix, etc) – adviseren bij wijzigingsvoorstellen – melden van beveiligingsprobleem aan security officer (escalatie niveau 2)
Security officer	– opstellen en onderhouden firewall security policy – goedkeuren changes – melden beveiligingsprobleem aan externe instanties (wettelijke of bedrijfsspecifieke verplichtingen) – opdrachtgever voor periodieke onafhankelijk audits (zoals penetratietesten) – melden van beveiligingsprobleem aan manager (escalatie niveau 3)

Bij nood- of escalatieregelingen mogen de functiescheidingen alleen worden doorbroken door de hogere managementlaag, waarbij dit meteen schriftelijk wordt vastgelegd. Na afloop van de calamiteit wordt onafhankelijk nagegaan of er geen inbraak heeft plaatsgevonden en of de functiescheiding ten volle hersteld is (bijvoorbeeld door het wijzigen alle wachtwoorden).

Een veelvoorkomend probleem is het consistent houden van de beschrijving en de implementatie van de firewall-policy. Vanuit de bedrijfsprocessen wordt grote druk gelegd op het oplossen van problemen of het realiseren van vereiste functionaliteit. Het werkend krijgen van zaken krijgt vaak ten onrechte een hogere prioriteit dan het handhaven en toetsen van het beveiligingsbeleid of de firewall-policy.

Dit risico wordt groter naarmate de firewall-policy meer veroudert. Het is daarom belangrijk om de firewall-policy als een 'levend document' te onderhouden met behulp van feedback van de beheerpartij, audits, de eigen gebruikersorganisatie en een regelmatige review van de risicoanalyse die aan de firewall-policy ten grondslag ligt. Op deze wijze kan men adequaat omgaan met veranderingen in de organisatie, veranderde behoeftes en nieuwe technologieën.

7.3 Beleggen beheer: intern of uitbesteden

Er zijn meerdere mogelijkheden om het operationele beheer van een firewall in te richten. De uiteindelijke vorm wordt bepaald door het besluit hoe met de beheerrisico's om te gaan. Te denken valt aan risico's die te maken hebben met de kosten, de beheerinspanning, het onderhouden van voldoende kennis, de afhankelijkheid van derden of het uit handen geven van bedrijfskritische informatie.

Er zijn een viertal mogelijkheden hoe met risico's om te gaan: accepteren, minimaliseren, ontwijken of overhevelen. Bij het overhevelen van risico's kan bijvoorbeeld gedacht worden aan het afsluiten van verzekeringen of het overdragen van bepaalde activiteiten aan derden. Wij onderscheiden twee hoofdlijnen bij het uitvoeren van beheeractiviteiten: 'zelf doen' of 'uitbesteden'. Binnen deze hoofdlijnen zijn veel varianten en mengvormen mogelijk. In de security policy wordt aangeven welke verantwoordelijkheden bij de organisatie zelf moeten blijven en welke eventueel overgedragen kunnen worden.

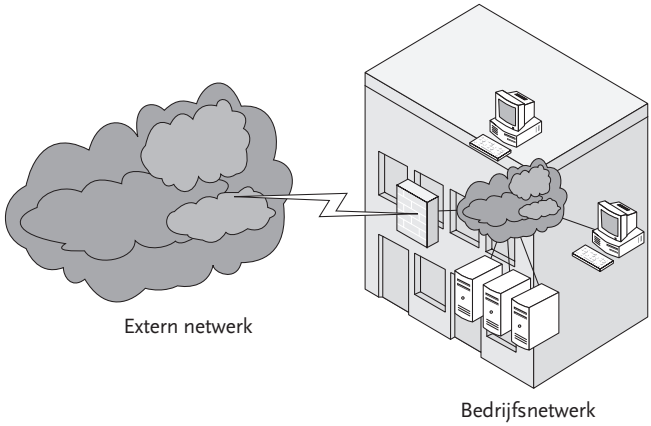
Zelf doen

Traditioneel leggen veel ondernemingen het beheer van informatiesystemen en infrastructuur inclusief beveiliging neer bij een interne beheerorganisatie. Deze vorm is relatief eenvoudig te realiseren en kan, mede door de korte communicatielijnen, een flexibele aanpak van beheren opleveren. De infrastructuur van deze oplossing is weergegeven in figuur 7.1.

Nadelen van 'zelf doen' is dat de organisatie geconfronteerd wordt met extra overheadkosten. De organisatie is zelf verantwoordelijk voor het borgen en controleren van de kwaliteit, de beschikbaarheid en de betrouwbaarheid van de firewall. Dit betekent dat er voldoende gekwalificeerd beheerpersoneel aanwezig moet zijn. Daarmee gaan hoge personeels- en opleidingskosten gepaard doordat gespecialiseerde vakkennis nodig is voor het beheer van de firewall-oplossing.

Uitbesteden

Door het groeiende aantal bedreigingen op internet en de toenemende complexiteit van de risico's en beveiligingsmaatregelen zien steeds meer organisaties zich genoodzaakt het operationele beveiligingsbeheer uit te besteden aan een gespecialiseerde partij, aan MMS, een *managed security services*-provider. Deze aanpak kan belangrijke voordelen opleveren.



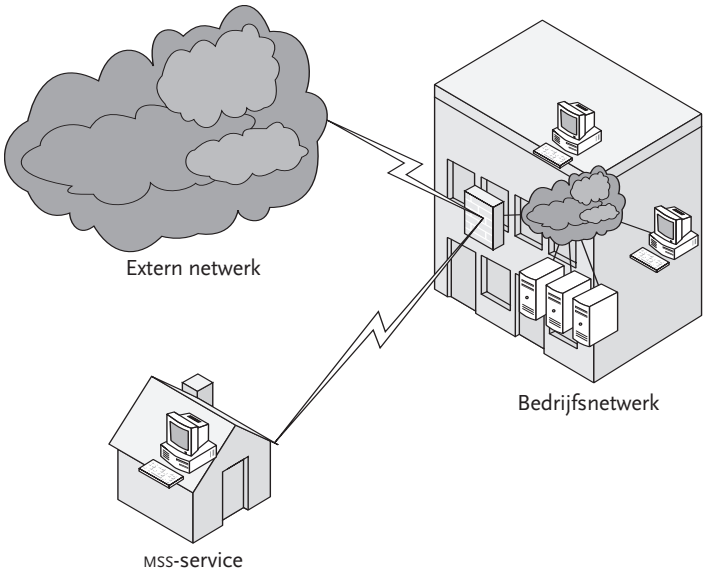
Figuur 7.1 Intern beheer

Een voorbeeld van een dergelijk voordeel is kostenreductie, omdat een MMS-provider zijn kosten voor faciliteiten, techniek, licenties en personeel kan spreiden. Waardoor 7 keer 24 uur monitoring makkelijker te realiseren is. Ook de beschikbaarheid van beveiligingsexpertise van de MMS-provider is een groot voordeel. Nadelen van MMS zijn de afhankelijkheid van de MMS-aanbieder, doordat het operationele beheer buiten de eigen organisatie plaatsvindt, en het uit handen geven van bedrijfskritische informatie. Daarom worden hogere eisen gesteld aan de afspraken die worden vastgelegd in een *service level agreement* (SLA).

Twee mogelijke varianten voor uitbesteden worden hier toegelicht.

Remote-beheer en monitoring (managed security services)

Bij managed security services wordt het beheer en de bewaking van de firewall uitbesteed terwijl de firewall binnen de eigen organisatie blijft (voor de afbeelding van de infrastructuur zie figuur 7.2). De MMS-provider heeft dan toegang tot de server en kan de logs en alerts van de fire-

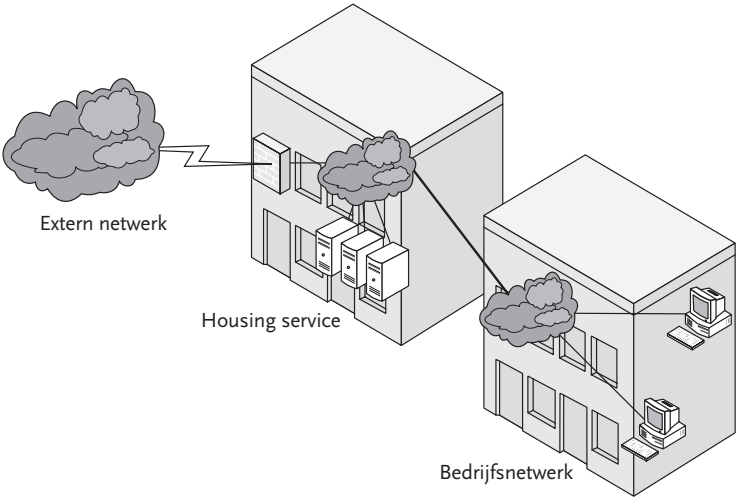


Figuur 7.2 Monitoring

wall in de gaten houden. Daarnaast heeft de MMS-provider de mogelijkheid om de rulebase aan te passen en de noodzakelijke updates uit te voeren. De organisatie ontvangt rapportages over uitgevoerde werkzaamheden en eventuele beveiligingsincidenten.

Veilige internetverbinding ('schone kabel')

Bij een 'schone kabel' is het volledige beheer van de firewall inclusief hardware uitbesteed aan een MMS-provider. De organisatie krijgt hiermee alleen schone en veilige gegevens binnen. De MMS-provider verzorgt netwerkfiltering, contentfiltering, anti-virus, *spam*-blokkade en incidentbeheer inclusief forensische analyse. De infrastructuur van deze oplossing is weergegeven in figuur 7.3.



Figuur 7.3 Schone kabel

7.4 Processen voor dagelijks onderhoud en beheer

Na de uitgangspunten beschreven te hebben op basis waarvan een firewall kan worden ingericht, zijn de processen aan de beurt die moeten zorgen voor het blijvend goed functioneren van deze component.

7.4.1 Configuratiebeheer (configuration management)

Configuratiebeheer heeft tot doel het onder controle brengen van de IT-infrastructuur en het beschikbaar stellen van informatie over de IT-infrastructuur. Hierbij worden configuratie-items gedefinieerd waarvan de status wordt vastgelegd. Iedere wijziging in de IT-infrastructuur leidt tot een wijziging in de status van één of meer configuratie-item(s).

Omdat een firewall een belangrijk IT-systeem is, moet een hoog detailniveau nagestreefd worden bij de vastlegging van de firewall-configuratie-items. Zo zal de status (inhoud) van de rulebase vastgelegd moeten zijn, waaruit duidelijk blijkt waarom specifieke regels in de rulebase staan. Veel firewalls beschikken over de mogelijkheid om een rapport te genereren waarin de instellingen van de rulebase beschreven staan, inclusief de reden waarvoor voor deze instelling is gekozen.

Naast de inhoud van de rulebase zijn firewall-versie en het patchlevel van belang. Eventueel kan gebruik worden gemaakt van specifieke tools, die de status en de wijzigingen van een firewall vastleggen en archiveren. Wijzigingen van configuratie-items moeten altijd plaatsvinden onder het toeziend oog van het wijzigingsbeheer.

7.4.2 Wijzigingsbeheer (change management)

Bijzondere aandacht is nodig voor het afhandelen van beveiligingsincidenten rondom de firewall en het verlenen van autorisaties voor firewallwijzigingen.

Voor het in stand houden van een adequaat beveiligingsniveau moet beheer actief op de hoogte blijven van nieuwe dreigingen. Hierbij kan de hulp worden ingeroepen van externe partijen, zoals de nationale *Computer Emergency Response Teams* (CERT's) of leveranciers. Nieuwe dreigingen zullen wijzigingen van de firewall, bijvoorbeeld in de vorm van updates, tot gevolg hebben. Het wijzigingsproces kan ook in gang gezet worden door het in gebruik nemen van nieuwe applicaties of het wijzigen van bestaande applicaties – sommige applicaties gebruiken bij-

voorbeeld eigen client/server-protocollen en hebben daardoor eigen openingen in de firewall nodig.

De meest voorkomende wijziging van een firewall is een aanpassing in de rulebase. Deze aanpassing kan het gevolg zijn van een wens (nieuwe functionaliteiten), een probleem (*vulnerability* of bug) of regulier proactief beheer (versimpeling van de rulebase).

De afhandeling van de wijzigingen wijkt voor een deel af van het reguliere *change proces*. De technische beoordeling van de wijzigingen wordt gedaan door de firewall-beheerder, die controleert op impact, risico en benodigde middelen (tijd en geld). Dan wordt de aanvraag getoetst aan de opgestelde firewall-policy. Indien het wijzigingsvoorstel hiervan afwijkt, dient de security officer autorisatie te verlenen.

Urgente noodwijzigingen (bijvoorbeeld veroorzaakt door incidenten) die niet het reguliere probleem- en wijzigingsproces hebben gevolgd, moeten achteraf alsnog via de gebruikelijke procedures worden goedgekeurd. In het proces zijn hiervoor de waarborgen geschapen in de vorm van scheiding tussen uitvoering en toezicht, interne controle achteraf (aan de hand van logging) en vastlegging van alerts (onafhankelijk van de beheerders).

Aanvragen dienen gearchiveerd te worden, zodat altijd bekend is waarom een wijziging in de rulebase is doorgevoerd, voor wie deze is doorgevoerd en eventueel zelfs tot wanneer deze wijziging actief moet zijn.

Firewall-rulebase

De firewall beschikt over een rulebase waarin wijzigingen worden doorgevoerd. Moderne firewalls bieden oplossingen voor versiebeheer en navolgbaarheid; wie heeft wat en op welk moment gewijzigd? Tevens kan een geavanceerde firewall ondersteuning bieden aan simpele *rollback*-mogelijkheden of *read-only*-toegang verschaffen tot de rulebase, bijvoorbeeld voor audits. Hierbij dient men er rekening mee te houden dat de firewall-rulebase niet de firewall-policy is, maar de uiteindelijke realisatie daarvan.

Documentatie

Een juiste wijze van verslaglegging van wijzigingen is cruciaal, omdat hiermee gewaarborgd wordt dat oude versies van de firewall-instellingen beschikbaar blijven en eventueel geraadpleegd of teruggezet kunnen worden.

Run-down (afbouw beheer)

Aan het eind van de levenscyclus van een firewall zal deze afgebouwd en opgeruimd worden. De geboden functionaliteit is dan overbodig of wordt door een andere functionaliteit overgenomen. De acties rondom deze afbouw zijn geborgd in het wijzigingsbeheer.

Omdat de informatie op een firewall een vertaling van het beveiligingsbeleid is, dient deze, voordat de firewall daadwerkelijk afgevoerd wordt, op de juiste wijze verwijderd te zijn. De hieronder beschreven acties dienen in de afbouw minimaal geregeld te zijn.

Waarborgen van het beveiligingsbeleid

De firewall vormt een onderdeel van de keten van beveiligingsmaatregelen die vanuit het beveiligingsbeleid zijn opgelegd. Het uitfaseren van een firewall leidt tot een wijziging in deze keten. Deze wijziging zal opgevangen moeten worden door nieuwe componenten, of anders doorgevoerd moeten worden in het beveiligingsbeleid.

Archivering/backup

De actuele status van de firewall dient veiliggesteld te worden, zodat een eventueel roll-back kan plaatsvinden. Daarnaast dienen logfiles beschikbaar te blijven voor analyse van eventuele (security-) incidenten.

Verwijderen van de bedrijfsgevoelige informatie

De firewall bevat een (deel van de) vertaling van het beveiligingsbeleid in de vorm van een rulebase. Deze data zijn bedrijfsgevoelig en dienen derhalve voor het afvoeren van de firewall verwijderd te worden.

Aanpassen van de documentatie/administratie

De actuele status van de firewall en de samenhang met andere componenten dient vastgelegd te zijn. Deze documentatie moet bij het verwij-

deren van de firewall aangepast en/of gearchiveerd worden. Voorbeelden hiervan zijn: netwerktekeningen, site-documenten, procedures en de configuratie-beheerdatabase.

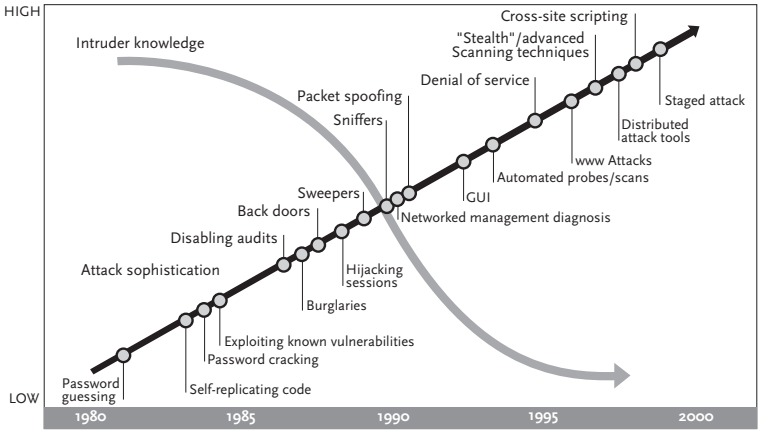
7.4.3 Incidentbeheer (incident management)

Naast het reguliere incidentbeheer, zoals de afhandeling van hard- en softwarestoringen, behelst het incidentbeheer van een firewall de afhandeling van beveiligingsincidenten. Hier ligt een van de belangrijkste taken van het firewall-beheer, namelijk het actief monitoren van de alerts en logs van de firewall. Hieruit kan afgeleid worden dat er zich een (dreigend) beveiligingsincident voordoet. Het is ook mogelijk dat incidenten via de servicedesk geïnitieerd worden. Meldingen van beveiligingsincidenten kunnen tenslotte ook van buiten de organisatie komen en escalatie van incidenten kan ook derden schaden (CERTS, ISP, Wetgever).

De helpdeskmedewerkers moeten goed weten welke criteria bepalen of een incident al dan niet een beveiligingsincident is. In geval van twijfel is het beter om een incident wél als beveiligingsincident te behandelen.

Beveiligingsincidenten houden zich zelden aan kantoortijden. Daarom wordt het vaak als noodzakelijk gezien om sleutelpersonen voor het afhandelen van beveiligingsincidenten permanent beschikbaar te hebben, hetzij door een 7 keer 24 uur bemand Security Network Operations Center, hetzij door het inrichten van telefonische stand-bydiensten.

Het toenemende computergebruik leidt tot een toename van het aantal beveiligingsincidenten (zie figuur 7.4). Zodra zich een beveiligingsincident voordoet, zal een organisatie snel en effectief moeten handelen. De snelheid van detecteren, acteren en oplossen van een beveiligingsincident bepaalt uiteindelijk de omvang van de inbraakschade, de impact en de benodigde kosten van herstel. De inzet van een Computer Emergency Response Team kan zorgen voor een snelle en effectieve aanpak van beveiligingsincidenten en kan tevens nieuwe beveiligingsincidenten voorkomen.



Figuur 7.4 Toename van incidenten

De taken van een CERT zijn:

- Reactief: een CERT handelt beveiligingsincidenten af en herstelt kwetsbaarheden.
- Pro-actief: een CERT kent een pro-actief beheer ter voorkoming van beveiligingsincidenten. Enkele taken: doorsturen van beveiligingsadviezen, onder de aandacht brengen van nieuwe technologische ontwikkelingen en opdracht geven voor een beveiligingsaudit.
- Gericht op beveiligingsmanagement: een CERT voert taken uit die indirect verband houden met beveiligingsincidenten. Denk bijvoorbeeld aan het geven van een bewustwordingstraining of het uitwerken van een calamiteitenplan.

Als blijkt dat een beveiligingsincident heeft plaatsgevonden, dan dient door onderzoek vastgesteld te worden wat de schade is en op welke wijze deze veroorzaakt is. Dit kan aanleiding zijn tot een forensische analyse door specialisten op dit gebied. Bij het afhandelen van een verstorend beveiligingsincident is er een groot spanningsveld tussen het enerzijds weer beschikbaar stellen van de omgeving en het anderzijds verzamelen van gegevens over het incident. Hierbij speelt de voorbereiding een sleutelrol: het direct beschikbaar hebben van (backup-)media om bewijsmateriaal veilig te stellen, de beschikbaarheid van de documentatie en soft-

ware om een schone installatie en een herstel van de instellingen uit te voeren en het geactiveerd hebben van logging om bewijsmateriaal te verzamelen.

Indien blijkt dat de oorzaak van het beveiligingsincident buiten de verantwoordelijkheid van het bedrijf ligt, kan worden overwogen aangifte te doen.

7.4.4 Uitwijk en calamiteitenbeheer (contingency management)

Backup/recovery

Omdat de firewall-configuratie als bedrijfsgevoelige informatie beschouwd kan worden, dient er extra aandacht geschonken te worden aan het transport en de opslag van deze configuratie, niet alleen tijdens het maken van een backup over het netwerk, maar ook tijdens het transporteren van de backup-media en tijdens de uiteindelijke vernietiging. Daarom moet de beheerorganisatie duidelijke instructies hebben voor het hanteren van media, en hier ook de benodigde faciliteiten voor kunnen gebruiken, zoals shredders, degaussers en software om harddisks te schonen.

Uitwijk/disaster recovery

Wanneer het risico van brand- of andere rampschade is afgevangen door het gebruik van een uitwijkscenario zullen ook hier procedures voor moeten zijn, waarin de rollen, verantwoordelijkheden, prioriteiten en activiteiten zijn beschreven. Deze procedures zullen periodiek getest moeten worden om te toetsen in hoeverre deze nog aansluiten bij de bedrijfsvoering, en om alle medewerkers voor te bereiden op een rampscenario.

7.4.5 Logging

Logging is het wegschrijven van informatie naar een logbestand, naar aanleiding van een gebeurtenis. Een log is een chronologische vastlegging van informatie, dat wil zeggen dat de (tijds)volgorde van het schrijven van informatie wordt weerspiegeld in een log. Het doel van logging

is het traceerbaar maken van gebeurtenissen en handelingen. Door het bijhouden van een log wordt het mogelijk te achterhalen wanneer iets gebeurde en wie verantwoordelijk was.

Logging kan in verschillende beheerprocessen gebruikt worden. De mate van logging moet in overeenstemming zijn met het doel. Voor incidentanalyse dient zoveel mogelijk gelogd te worden, terwijl voor rapportage volstaan kan worden met het loggen van de hoofdlijnen van het netwerkverkeer. Om de logfiles overzichtelijk en hanteerbaar te houden, dienen ze op regelmatige basis geroteerd en gearchiveerd te worden.

Op basis van de informatie in een log is het mogelijk onderzoek naar handelingen en gebeurtenissen te doen. In beveiligingsbewuste organisaties zal inspectie van logbestanden worden uitgevoerd door andere medewerkers dan de firewall-beheerders.

Let er op dat het registreren van gebeurtenissen in een logbestand onderworpen zal zijn aan de Wet op de Bescherming van Persoonsgegevens. Dat beperkt de gebruiksmogelijkheden. Registratie in een logbestand is wel vrijgesteld van de meldingsplicht op grond van de wet. Die vrijstelling is geregeld in (onder meer artikel 33 van) het Vrijstellingsbesluit. Van belang is wel de doelbinding: de registratie mag uitsluitend worden gebruikt voor de in de wet omschreven doelen.

Het gebruik van de loggegevens voor andere doeleinden is mogelijk (bijvoorbeeld voor het vaststellen van misbruik door personeel), mits afdoende geregeld in protocollen, die onder meer met ondernemingsraden zijn besproken. Bovendien zal logginganalyse regulier en op objectieve grondslagen moeten plaatsvinden. Logging wordt echter niet zonder meer automatisch geaccepteerd als bewijsmateriaal in gerechtelijke procedures.

Analyses om misbruik door personeel vast te stellen, mogen uitsluitend op statistische wijze worden uitgevoerd (door niet-geïndividualiseerde methoden). Pas bij sterke vermoedens van misbruik zou specifiek onderzoek een optie zijn. Een en ander moet formeel vastgelegd zijn. Ook het sanctiebeleid moet eenduidig zijn en, net als de protocollen, bekend zijn bij het personeel.

7.5 Eisen aan beheerders

De bovengenoemde punten stellen hoge kwaliteitseisen aan de beheerders. Op procedureel niveau dient men voldoende bekend te zijn met het beveiligingsbeleid. Het personeel dient voldoende bekend te zijn met de afgeleide procedures. Daarnaast dient het firewall-personeel voldoende technische kennis te hebben van de firewall-infrastructuur en de aangrenzende componenten, om een goed oordeel te kunnen vellen over eventuele risico's rondom wijzigingen in de infrastructuur en de omgeving.

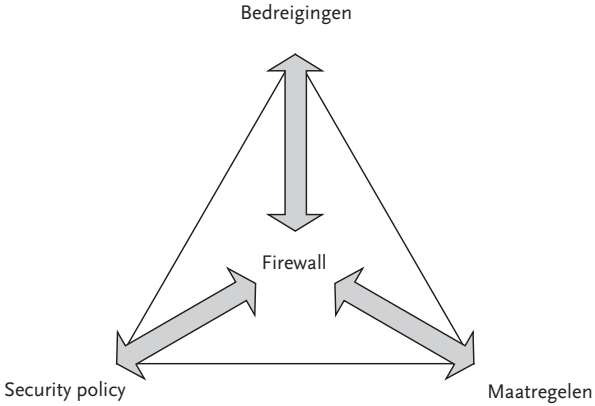
Een additionele eis aan de firewall-beheerder is dat hij of zij met bedrijfsgevoelige informatie om kan gaan. In voorkomende gevallen kan de organisatie ervoor kiezen een antecedentenonderzoek te verrichten naar personen die deze rol gaan vervullen.

De technologie (applicatie en hardware) van een firewall is voortdurend in ontwikkeling. Deze bestaat enerzijds uit nieuwe mogelijkheid, anderzijds uit verbeteringen. De verbeteringen (patches en fixes) zijn vaak een noodzakelijk kwaad waarin een firewall mee moet groeien, omdat hiermee kwetsbaarheden worden gedicht.

De firewall-beheerder zal zich, vanwege zijn beherende maar ook adviserende rol, permanent moeten informeren en bijscholen op het gebied van nieuwe ontwikkelingen, bedreigingen en eventuele policy-veranderingen in de organisatie.

7.6 Audits

De firewall als object wordt beïnvloed door wijzigingen in bedreigingen, het beveiligingsbeleid en maatregelen. Door deze wijzigingen moet de firewall ook veranderen. De relatie van de firewall met het beveiligingsbeleid, de bedreigingen en de maatregelen is weergegeven in figuur 7.5.



Figuur 7.5 Relatie firewall, bedreigingen, beveiligingsbeleid en maatregelen

Meer dan bij andere delen van de infrastructuur behoren firewall-audits tot de reguliere instrumenten van het beheer. Na alle grote wijzigingen dient de consistentie van de firewall middels een audit getoetst te worden.

Bij een security-audit is het van belang om vooraf de doelstelling van de audit duidelijk te stellen. Een gebruikelijke auditdoelstelling is het vaststellen dat de vertrouwelijkheid, integriteit en beschikbaarheid van de firewall en het netwerk daarachter niet geschaad kunnen worden. Vooral de beschikbaarheid, of beter gezegd het onbeschikbaar maken van de firewall, is vaak een doel voor hackers.

Bij een firewall-audit kunnen in hoofdlijnen twee benaderingen worden gevolgd. De ene benadering richt zich op de processen rond het beheer, waarbij objecten zoals techniek, procedures, organisatie en beleid aan een onderzoek worden onderworpen. De tweede, meer specifieke, benadering is de penetratietest, waarbij geprobeerd wordt de beveiliging te doorbreken. De penetratietest kan zowel vanuit intern als extern perspectief uitgevoerd worden, en zowel de benadering van de *crystal box* (met alle informatie over de infrastructuur) als die van de de *black box* (zonder informatie over de infrastructuur) kunnen worden gebruikt.

Daarnaast kan men er binnen de organisatie waar de penetratietest wordt uitgevoerd, voor kiezen geen ruchtbaarheid aan deze test te geven (*red team*). Vaak zal dan slechts één persoon of een heel beperkte kring op de hoogte zijn van de penetratietest. Een red team benadert dus het dichtst een 'echte' aanval op de beveiliging. Als er sprake is van een *green team*, dan is men op grotere schaal op de hoogte van de penetratietest. Dit gaat dan meer in de richting van een audit. In zo'n geval is het dan ook de vraag of men binnen de organisatie op dezelfde wijze reageert als in het geval van een echte aanval. Men is immers op de aanval voorbereid en weet dat het een 'onschuldige' aanval betreft.

Aan het uitvoeren van penetratietesten zijn risico's verbonden. Er dienen dan ook strikte afspraken gemaakt te worden over doel en grenzen, aansprakelijkheden, randvoorwaarden en geheimhoudingsverklaringen. Het uitvoeren van penetratietesten is overigens een activiteit die veel specifieke expertise vraagt, wil deze een zinvol resultaat opleveren. Daarom worden penetratietesten vaak uitbesteed aan daarin gespecialiseerde bedrijven.

8 Basisnormen en basismaatregelen

Aan de PI-studie *Basisnormen Beveiliging en Beheer IT-Infrastructuur* kan een aantal basisnormen worden ontleend, die specifiek betrekking kunnen hebben op firewalls. Wij recapituleren deze hieronder, omdat ze input hebben gevormd voor nadere uitwerking in deze studie. Wij merken op dat de basisnormen in sommige gevallen een ruimere reikwijdte hebben, zodat niet alle elementen in de PI-studie *Firewalls* aan de orde komen. Ook kan worden geconstateerd dat voortschrijdend inzicht leert dat deze basisnormen beter kunnen worden afgestemd op de firewallstudie. Hiermee zal rekening worden gehouden bij het onderhoud van deze basisnormen.

Bij de basisnormen wordt tussen haakjes het corresponderende paragraafnummer gegeven van de PI-studie *Basisnormen Beveiliging en Beheer IT-infrastructuur*.

8.1 Basisnormen IT-infrastructuur, specifiek voor firewalls

Architectuur (3.1.1)

1 Bij de inrichting van de IT-infrastructuur wordt onderscheid gemaakt naar domeinen, die elk een eigen beveiligingsniveau hebben, waarbij van elk domein is bepaald welke onderling samenhangende elementaire technische en procedurele beveiligingsmaatregelen zijn getroffen. Bepalend voor het onderscheid naar domeinen is onder meer:
   a het algemene beleid inzake beveiliging;
   b het beveiligingsbelang van de toepassingen en de gegevens;

c de beheer- en beveiligingseigenschappen van de platforms;
d het onderscheid naar ontwikkeling, acceptatietest, productie en beheer;
e de toegankelijkheid tot gegevens en servers voor internen en externen (zoals het publiek);
f de wijze waarop de omgevingen worden beheert (bijvoorbeeld beheer door eigen organisatie, beheer uitbesteed, beheer door onvertrouwde omgeving zoals internet of door een testomgeving voor technische infrastructuur (TIS)-componenten).

Filterende netwerkkoppelingen (3.5)

1 Bij de inrichting van de IT-infrastructuur is afgewogen welke maatregelen kunnen worden getroffen om het dataverkeer tussen de domeinen te beperken en te beheersen. Methoden die zowel uit beheer- als beveiligingsoogpunt kunnen worden toegepast, zijn:
a scheiding van het netwerk op fysiek niveau door aparte kabels, patchkasten et cetera, in combinatie met fysieke overdracht via verplaatsbare opslagmedia;
b het toewijzen van vaste lijnen of telefoonnummers;
c het automatisch verbinden van poorten aan bepaalde toepassingssystemen of beveiligingsgateways;
d het gebruik van specifieke toepassingsystemen en/of beveiligingsgateways verplicht stellen voor externe gebruikers;
e actief beheer van de verbindingen tussen toegestane bronnen en communicatiemiddelen, door middel van beveiligingsgateways, bijvoorbeeld firewalls;
f *bridging*: alleen doorlaten dataverkeer van segment A naar segment B (en vice versa) dat voor het andere segment bedoeld is, zodat alleen het noodzakelijke dataverkeer van het andere segment zichtbaar wordt binnen het eigen segment (en vice versa);
g *switching*: hierbij kan een willekeurig aantal netwerksegmenten logisch van elkaar worden gescheiden (onzichtbaar gemaakt);
h *virtual LAN*: een uitgebreide versie van switching, hierbij kunnen (fysieke) netwerkadressen worden gegroepeerd tot (logische) 'werkgroepen', vervolgens wordt het verkeer van één werkgroep logisch onzichtbaar gemaakt voor de andere werkgroepen;
i *routing*: dataverkeer naar andere netwerken leiden door toeken-

ning van verschillende (blokken van) netwerkadressen; dataverkeer tussen de segmenten wordt verzorgd door een parametriseerbare router die daardoor ook bepaalde niet-geautoriseerde communicatiestromen kan blokkeren;

j *protocollen*: op verschillende segmenten wordt een verschillend netwerkprotocol gebruikt, waardoor de segmenten elkaars datastromen niet kunnen lezen; communicatie tussen segmenten vindt plaats via gateways die protocollen kunnen omzetten;

k *tunneling*: door middel van versleuteling op systeemniveau kan een datastroom onleesbaar gemaakt worden (bijvoorbeeld de toepassing van een *virtual private network*); op dit moment wordt deze techniek voornamelijk gebruikt voor dataverkeer over internet, maar zij is ook toepasbaar binnen een bedrijfsnetwerk;

l *cryptomodems*: voor versleuteling van datastromen;

m *op toepassingsniveau via public key infrastructures* (PKI's): met encryptiemethoden de uitwisseling van gegevens over netwerken beveiligen en de identiteit van de communicerende partijen authenticeren (zie hiervoor ook *Technische Beveiligingsstudie Encryptie* van het Platform Informatiebeveiliging);

n *firewall/guard*: blokkeren van ongewenst dataverkeer, hierbij kan op meer kenmerken worden geselecteerd, zoals: afzender, protocol, poort, soort verkeer, inhoud gegevens, et cetera (zie hiervoor ook de PI-studie *Internet*).

Het valt buiten het kader van deze PI-studie om alle details en keuzemogelijkheden te beschrijven. Als richtlijn kan worden aangegeven dat een oplossing moet worden gekozen die voldoet aan de onderstaande criteria. Dit is geen triviaal probleem omdat de verschillende criteria strijdig zijn:

a de oplossing moet in de praktijk beproefd zijn en moet voldoen aan alle eisen (*proven technology*);

b de oplossing moet gebruikmaken van gestandaardiseerde componenten, zodat incompatibiliteitsproblemen worden vermeden;

c de oplossing moet aansluiten bij de organisatorische structuur (afdelingen, functiescheiding) en de geografische structuur (vestigingen, regio's);

d de oplossing moet aansluiten bij de externe klantstructuur (geografisch, extranet of publiek);

e de oplossing moet zo veel mogelijk aansluiten bij de mogelijkheden van de bestaande IT-infrastructuur binnen de organisatie;
f de oplossing moet het gewenste beveiligingsniveau binnen ieder domein van de IT-infrastructuur waarborgen, ook als binnen sommige domeinen van de IT-infrastructuur een extra hoog niveau vereist is;
g de beheersinspanning moet beperkt zijn, ook bij reorganisaties en verhuizingen.

2 Een filterende netwerkkoppeling met een onvertrouwd domein, zoals internet, voldoet aan de volgende richtlijnen:
a bestaat altijd uit ten minste twee onafhankelijke en ongelijksoortige filterende apparaten die na elkaar worden doorlopen, bijvoorbeeld een router met daarachter een proxy;
b maakt gebruik van tenminste één DMZ (de-militairized zone, het gebied tussen de twee onder punt a genoemde filterende apparaten);
c past Data Name Server/Network Address Translation toe in verband met beperkt zichtbaar maken van de interne structuur van het vertrouwde domein;
d past maatregelen toe op het gebied van anti-virus en intrusion detection;
e onderbreekt zonodig sessies bij openstaande verbindingen om denial-of-service-aanvallen af te slaan;
f maakt gebruik van proxy en *reversed*-proxy;
g biedt faciliteiten voor versleutelde sessies;
h beëindigt tunnels op de filterende netwerkkoppeling teneinde contentscanning en intrusion detection mogelijk te maken;
i maakt voor het uitvoeren van beheerhandelingen alleen gebruik van een daarvoor bestemde netwerkinfrastructuur;
j maakt gebruik van een onderliggende TIS die zoveel mogelijk ontdaan is van faciliteiten die niet strikt noodzakelijk zijn voor het functioneren van de filterende netwerkkoppeling. Wanneer dat niet mogelijk, moeten alle niet strikt noodzakelijke faciliteiten van de TIS worden uitgeschakeld. Dit alles om de kans op misbruik van deze onnodige faciliteiten tot een minimum te beperken (stripping/hardening).

3 Er is bepaald welke soorten datatransporten of data-transportfaciliteiten op welke momenten door de filterende netwerkkoppeling mogen worden doorgelaten. Alle datatransporten die niet aan deze voorwaarden (filterfuncties) voldoen worden geblokkeerd. Voorbeelden van filterfuncties:
   a alleen expliciet goedgekeurde protocollen (bijvoorbeeld e-mail) worden doorgelaten;
   b datatransporten of te transporteren bestanden met een niet-leesbare inhoud of een mogelijk gevaarlijke inhoud (virussen) worden geblokkeerd;
   c bestandsoverdracht in één richting of in beide richtingen wordt geblokkeerd;
   d toegang tot het 'achter' de filterende netwerkkoppeling liggende netwerk is afhankelijk van tijdstip of datum.

8.2 Basismaatregelen techniek firewalls

Architectuur

1 In de analysefase van het architectuurontwerp is vastgesteld welke domeinen als onderdeel van de technische infrastructuur te onderscheiden zijn.
2 Op basis van de vertrouwensmatrix is vastgesteld tot welk vertrouwenstype de onderkende domeinen behoren.
3 Op basis van een analyse van datastromen tussen de onderkende domeinen, de vertrouwenstypering hiervan en het verschil in beveiligingsniveau is in algemene zin vastgesteld welke firewall-functionaliteiten deel moeten uitmaken van de filtering tussen de onderkende domeinen.
4 Op basis van een analyse van de aard van de verbindingen en bijzondere domeinsituaties zijn nadere verfijningen in de filtering vastgesteld.

Implementatie

5 Bij de nadere invulling van het ontwerp van de firewall wordt een juist evenwicht bewaard tussen centralisatie en decentralisatie van koppelingen op knooppunten teneinde centrale complexiteit niet ten koste te laten gaan van overzicht en beheersbaarheid.

6 De firewall kent geen componenten, die een single point of failure kunnen betekenen voor het geheel. Redundante componenten worden ondersteund door een backup/recovery-strategie.
7 Excessieve belasting van de ene informatiestroom heeft geen onaanvaardbare gevolgen voor de andere stromen (load balancing).
8 Het beheerverkeer loopt via een ander netwerk dan het productieverkeer (out-of-bandmanagement).
9 Apparatuur en besturingssystemen zijn ontdaan van onderdelen of functionaliteiten die kwetsbaarheden kunnen bevatten (hardening).
10 Ingeval er geen persoonsgebonden user accounts voor beheerders worden geboden in de firewall-configuraties, worden hiervoor aparte oplossingen gehanteerd, zoals bijvoorbeeld een terminal concentrator.
11 Er zijn voldoende extra maatregelen getroffen voor het transport en de opslag van de firewall-backups in verband met de gevoelige informatie die ze bevatten en de mogelijk onveilige protocollen waarmee ze getransporteerd worden.
12 Toegangsregels in de rulebase worden gegroepeerd ten behoeve van de overzichtelijkheid.
13 Bij firewall-producten, waarbij de rulebase sequentieel wordt doorlopen (geen database), worden de regels die het meest gebruikt zullen worden zo hoog mogelijk in de rulebase opgenomen.
14 Bij toepassing van een cut through-proxy is het risico van meeliften door clients achter een webproxy niet van toepassing, onderkend en geaccepteerd of zijn er anderszins maatregelen getroffen om dit risico op te vangen.
15 False positives en false negatives geven door hun frequentie geen aanleiding tot het onvoldoende tijdig herkennen van de 'echte' alerts door voortdurende fine-tuning van de firewall.
16 In de technische documentatie van de firewall worden de achterliggende motivatie van de configuratieparameters, de samenhang met andere parameters en componenten en de samenhang met de security policy opgenomen.

Functionaliteit

17 *Rate limiting* wordt toegepast om DOS-attacks te voorkomen en om te trachten QoS te waarborgen.

18 Er wordt afhankelijk van het belang van de te filteren gegevens contentscreening toegepast door middel van een verantwoorde keuze uit black list en/of white list.

19 Er worden anti-spoofingtechnieken gebruikt om het afschermen of veranderen van de eigen identiteit bij het verzenden van berichten tegen te gaan.

20 Onnodige protocollen en onnodige datapakketten worden niet doorgegeven (bijvoorbeeld broadcastverkeer).

21 Bij toepassing van proxy, contentscanning en intrusion detection wordt standaard uitgegaan van toepassing van een de-militarized zone (DMZ) die aan beide zijden (aan de buitenste, *untrusted* zone en aan de binnenste *trusted* zone) wordt begrensd door netwerkcomponenten met beveiligingsfunctionaliteit.

22 Bij DMZ's is het uitgangspunt dat de beveiligingscomponenten aan beide zijden functioneel redundant zijn in die zin dat sprake is van technisch verschillende componenten.

23 In het kader van het garanderen van afgesproken beschikbaarheidniveaus worden routers zodanig ingesteld dat zij bij uitval van een verbinding een andere route kiezen en het dataverkeer omleiden. Een dergelijke dynamische routering wordt alleen binnen een intranet toegepast. Koppelingen naar externe netwerken verlopen altijd door middel van een statische routering.

24 Er wordt voor gezorgd, daar waar mogelijk, dat interne routeringinformatie alleen intern op het netwerk beschikbaar is. Het uitwisselen van routeringinformatie zou alleen mogelijk moeten zijn tussen wederzijds geauthenticeerde routers.

25 Versleutelde verbindingen eindigen zodanig op de firewall dat contentscanning kan plaatsvinden. Afwijkingen op deze regel zijn expliciet goedgekeurd door de security officer nadat de risico's door hem zijn beoordeeld.

26 Standaard beheertools die voorzien in gelijktijdige communicatie in twee richtingen worden bij voorkeur niet gehanteerd. Bij voorkeur ook geen twee-wegcommunicatie bij applicaties (bijvoorbeeld FTP).

27 Logfiles verstrekken gegevens over de volgende drie categorieën:
   a kritieke systeemproblemen: hardware- en softwarefalen;
   b administratieve gebeurtenissen: geautoriseerde acties op het terrein van firewall-rulebasewijzigingen, systeem-configuratiewijzigingen, account(autorisatie)wijzigingen; alle *dropped packets*, afgewezen verbindingen en *rejected attempts*, tijd, protocol en gebruikersnaam voor alle succesvolle connecties door de firewall,
   c netwerkverbindigen: verbindingen die geaccepteerd of geweigerd worden, afwijkende verbindingsaanvragen.

   In het geval van afwijkende verbindingsaanvragen bevat de logging ten behoeve van eventuele bewijsvoering bij strafrechtelijke vervolging de volgende gegevens:
   – per regel: datum en tijd van het optreden van de gebeurtenis;
   – van elke totstandgekomen sessie: source-IP-adres, destination-IP-adres en protocol en poort;
   – het benaderen van een niet geopende poort;
   – het benaderen van een op de gezochte poort niet geactiveerde dienst;
   – het benaderen van een poort met een niet bij voorbaat daarvoor bestemd programma of protocol;
   – het uitvoeren van de alert-functie door de firewall;
   – het met behulp van toegestane protocollen en programmatuur uitvoeren van ongewenste activiteiten (het opgeven van besturingsparameters, bijvoorbeeld het in een commando opgeven van een *pipe*-symbool);
   – het geautoriseerd en ongeautoriseerd toegang krijgen tot de configuratie van de beveiligingscomponent (parameterinstellingen, rules, management information base, et cetera);
   – modificatie van access control-permissies voor gebruikers en security-parameters (unsuccessful en successful);
   – IP-adressen, als er bijvoorbeeld poorten of services nodig zijn voor het beheer van de firewall dan dient er een rule te worden opgenomen in de rulebase voor het beperken van de toegang tot deze poorten;
   – foutmeldingen van routers, *bastion host* en proxyingprogramma's.

28 Gelogde gegevens dienen een beperkte periode na registratie on line en daarna off line beschikbaar te zijn voor analyse achteraf en het afleggen van verantwoording in het kader van interne controle.
29 Een real-time logginganalyse of intrusion detection-systeem:
   a analyseert permanent of er inbraakpogingen worden gedaan;
   b is in staat terstond een alert-functie aan te roepen om de beheerders direct op de hoogte te stellen van een inbraak(poging);
   c zou in staat moeten zijn om op basis van een analyse een verbinding te beëindigen;
   d mag zelf geen beveiligingsrisico vormen.
30 Het verdient de voorkeur het logbestand op een andere dan de loggende component op te slaan en hierbij gebruik te maken van authenticatie.
31 Voor beheer wordt bij voorkeur gebruik gemaakt van beveiligde diensten als SSH.
32 Bij het inzetten van DNS in combinatie met een firewall worden de volgende basisregels gevolgd:
   a gebruik van de laatste versie DNS-software;
   b uitwisseling van zone-data alleen met geautoriseerde DNS-servers;
   c zo mogelijk gebruik van een 'split- DNS-infrastructuur'.

8.3 Basisnormen beheerprocessen, specifiek voor firewalls

Inrichting processen (4.1)

1 Bij nood- of escalatieregelingen mogen de functiescheidingen alleen worden doorbroken door de hogere managementlaag, waarbij dit onverwijld schriftelijk wordt vastgelegd. Na afloop van de calamiteit wordt onafhankelijk nagegaan of er geen compromittering heeft plaatsgevonden en of de functiescheiding (bijvoorbeeld een wijzigen alle wachtwoorden) ten volle hersteld is.
2 Binnen de beheerprocessen zijn de bevoegdheden bij incidenten voor het tijdelijk onderbreken van de serviceverlening, het communiceren met anderen binnen de exploitatieorganisatie en met de

klantorganisatie, evenals het in gang zetten van nood- of escalatieprocedures eenduidig. Deze bevoegdheden zijn niet strijdig met bevoegdheden van het lijn- en/of procesmanagement.

Incident management (4.9)

1 Van elke oplosgroep zijn de verantwoordelijkheden (aandachtsgebieden) en bevoegdheden (onder andere mogelijkheden voor inschakelen leveranciersondersteuning) bepaald.
2 Voor het afhandelen van urgente en niet-standaard beveiligingsincidenten (bijvoorbeeld bij computervirusinfecties en aanvallen via internet) fungeert een aparte oplosgroep, een CERT (Computer Emergency Response Team) met vertegenwoordiging van security management.
3 Bij (een vermoeden van) het overtreden van beveiligingsregels wordt er tijdig bijzondere aandacht besteed aan het veiligstellen van bewijzen (loggegevens, opdrachten en dergelijke) en het doen van aangifte.
4 De beschikbaarheid en bereikbaarheid van oplosgroepen is geborgd. Hierbij wordt speciale aandacht geschonken aan de beschikbaarheid en bereikbaarheid buiten kantooruren (stand-bydiensten).
5 Buiten het reguliere problem- en changeproces om aangebrachte noodwijzigingen, als gevolg van incidenten met een bijzonder (urgent) karakter, doorlopen achteraf alsnog de gebruikelijke procedures. In het proces zijn hiervoor de waarborgen geschapen.

Problem management (4.10)

1 Er is vastgelegd wie en in welke situaties (bij welke klasse van problemen) bevoegd is om vanuit het problem management-proces een spoedeisende wijziging (*emergency change*) te initiëren.

Change management (4.11)

1 *Change requests* worden toegewezen aan change-categorieën. Hierbij geldt de volgende aanvullende norm:
   a aan elke categorie zijn specifieke afhandelingsprocedures gekoppeld, waarin onder meer is geregeld dat er voor spoedeisende changes een aparte procedure is waarbij eventueel achteraf het change-proces alsnog wordt doorlopen;

Operations (4.13)

(Pro-actief beheer TIS-componenten)

1 Door het systematisch raadplegen van leveranciersinformatie en informatie van (externe) CERT's wordt vastgesteld in hoeverre de eigen IT-infrastructuur zwakheden of beveiligingslekken vertoond.
2 Nieuwe releases en patches van TIS-componenten, onder andere wegens zwakheden en beveiligingslekken, worden tijdig geïnstalleerd.
3 Bij patches, die vanaf internet worden gedownload, wordt gecontroleerd of met de juiste internetsite contact is gelegd en/of wordt het gebruik van digitale handtekeningen geverifieerd.

8.4 Basismaatregelen beheer firewalls

De basisnormen zijn in veel gevallen al dermate gedetailleerd geformuleerd, dat we deze niet gaan herhalen, maar alleen nader zullen invullen voorzover hoofdstuk 7 daartoe aanleiding geeft. Dit betekent dat de set basismaatregelen in dit onderdeel alleen in combinatie met de basisnormen een dekkend geheel vormt.

1 Er is een firewall-policy opgesteld, die aansluit op de algemene policies voor beheer en beveiliging, en er zijn afspraken gemaakt in SLA's. In de policy zijn tenminste de volgende onderwerpen uitgewerkt:
   a aanduiding belang firewall voor bedrijfsprocessen en beveiliging;
   b betrokkenheid verschillende disciplines;
   c algemene verantwoordelijkheidsverdeling inclusief escalatieniveaus;
   d aanvraag, autorisatie en uitvoering van wijzigingen;
   e omgang met beveiligingsincidenten (speciale bevoegdheden, communicatie);
   f change control policy, spoed-changes;
   g organisatiewijze beheeractiviteiten;
   h CERT;
   i audits.

2 Er is functiescheiding tussen manager, helpdesk-/incidentmanagement, firewall-beheerder en security officer.
3 De firewall-policy wordt onderhouden naar aanleiding van grotere changes, de evaluatie van incidenten of veranderingen in de relevante omgeving.
4 Alle changes in de firewall die afwijken van de security policy worden door de security officer goedgekeurd.
5 De changes in de firewall worden systematisch gearchiveerd.
6 Er wordt periodiek vastgesteld of de loggingserver operationeel is.
7 In het personeelsbeheer wordt voldoende aandacht besteed aan eventuele screening van beheerpersoneel, functieroulatie, het vermijden van situaties waarbij ernstige ontevredenheid kan ontstaan en de zorg voor goede opleiding en ondersteuning.
8 Er is voor de firewall-omgeving een auditstrategie uitgewerkt, waarin de aard en planning van de toetsingen zijn afgestemd op risico's en wijzigingen met een evenwichtige verdeling van de auditmethoden.