

Firewall Technologie

whitepaper firewall technieken

**TUNIX keeps your
security up !**



1. De TUNIX organisatie

TUNIX houdt zich primair bezig met het voor haar klanten beheren van netwerkbeveiligingsoplossingen en heeft daarin een goede naam opgebouwd. TUNIX bouwt, levert, evalueert, beheert en zorgt voor het onderhoud van beveiliging-systemen.

Firewalls worden door TUNIX turn-key en dus volledig operationeel opgeleverd. Tot onze taken rekenen we daarom opleiding, advies, ontwerp, implementatie, coördinatie, plaatsing van de hardware, oplevering, overdracht en beheer. In de praktijk nemen wij dit soort projecten meestal in z'n geheel voor onze verantwoording en wordt de geïnstalleerde firewall middels een *Managed Firewall Service* SLA door TUNIX beheerd.

Op het gebied van beveiligingsoplossingen biedt TUNIX een breed dienstenpakket. Dat pakket bestaat uit productonafhankelijke opleidingen op het gebied van netwerktechnologie, netwerkbeveiligingsadvies, firewall-implementaties, VPN-oplossingen, beheer van firewall-systemen en zowel standaard- als maatwerk ontwikkelingswerkzaamheden.

De TUNIX beveiligingsoplossingen zijn modulair opgebouwd, wat het mogelijk maakt dat wij voor klanten die dat wensen, 3rd party componenten naadloos kunnen integreren.

De optionele modules die wij aanbieden bevatten technologie van 3rd parties (onze Technology Partners) zoals Kaspersky Labs, Cisco, F5, V-one, Rainbow, Vordel, Emerging Technologies, Secure Computing en anderen.

Contactinformatie

TUNIX is gevestigd op de volgende locaties:

- Het technisch centrum en N.O.C. bevindt zich in Nijmegen. De contactgegevens voor deze locatie zijn:

TUNIX Internet Security & Opleidingen	
Wijchenseweg 111	
6538 SW Nijmegen	
Telefoon algemeen:	+31 (24)3455000
Fax algemeen:	+31 (24)3455001



- Ons cursus-, presentatie- en verkoop-centrum bevindt zich in Veenendaal. De contactgegevens voor deze locatie zijn:

TUNIX Internet Security & Opleidingen	
Plesmanstraat 36	
3905 KZ Veenendaal	
Telefoon verkoop:	+31 (318)546300
Fax verkoop:	+31 (318)546303

Routebeschrijvingen voor deze locaties vindt u op onze website www.tunix.nl.



2. Overzicht firewall technieken

Dit white paper geeft in vogelvlucht een overzicht van algemene firewall technieken. In het white paper “TUNIX Security Portfolio” wordt een overzicht gegeven van producten en diensten die TUNIX aanbiedt.

Organisaties die een koppeling met het Internet willen maken dienen daarbij zorg te dragen voor een adequate beveiliging van het eigen netwerk. Dat kan door het opzetten van één of meer *firewalls*. Een firewall is een systeem of een groep van systemen waarmee op één of meer centrale punten een verdedigingslinie gevormd wordt tegen aanvallen vanuit de buitenwereld. Alle verkeer tussen de buitenwereld en het bedrijfsnetwerk verloopt via de firewalls en wordt onder controle van de firewalls doorgelaten of tegengehouden. Wanneer er geen gebruik gemaakt wordt van een firewall moet elke machine in het netwerk afzonderlijk tegen aanvallen beschermd worden, iets wat zeker in grotere netwerken ondoenlijk is en bovendien de functionaliteit van het bedrijfsnetwerk schaadt. Firewalls worden ook ingezet in het bedrijfsnetwerk om segmentatie te realiseren.

In dit white paper wordt beschreven hoe een firewall een bedrijfsnetwerk kan beveiligen tegen aanvallen vanuit het Internet. Het is als volgt opgebouwd: als eerste wordt uitgelegd hoe men te werk moet gaan bij het realiseren van een beveiligingsoplossing. Daarbij wordt een onderscheid gemaakt tussen het doel (de te realiseren beveiliging en functionaliteit) en het middel (de daarvoor ingezette firewall-technieken). Vervolgens wordt besproken wat het takenpakket van een firewall is en wat een firewall wel en niet kan doen: welke beveiligingsdoelen kunnen met behulp van een firewall gerealiseerd worden? Daarna worden firewall-technieken beschreven die beschikbaar zijn om de gestelde beveiligingsdoelen te realiseren.

2.1 De security-policy en de firewall

De eisen die gesteld worden aan een firewall volgen uit de *security-policy* van een organisatie. Deze legt vast wat de gewenste functionaliteit is en welke bescherming de firewall moet bieden. De security-policy ziet er in principe voor elk bedrijf anders uit, omdat elk bedrijf haar eigen specifieke wensen en toepassingen heeft. Er kan bijvoorbeeld sprake zijn van telewerkers die van buiten op een veilige manier in het bedrijfsnetwerk moeten kunnen inloggen, van Websurfers die gecontroleerd (bekijken ze niet teveel pagina's die niets met het werk te maken hebben?) gebruik mogen maken van Internet, van een bedrijf dat alleen email uitwisselt met het Internet, of van een organisatie die van alle denkbare nieuwe Internet-toepassingen (telefonie, videoconferencing) gebruik wil maken - maar wel op een veilige manier.



Uit het voorgaande blijkt dat elke situatie verschillend is: elk organisatienetwerk heeft zijn eigen karakteristieken wat betreft de gewenste toepassingen en de security-eisen. Een firewall is dan ook per definitie een op maat samengestelde set van componenten die tezamen de security-policy van een bedrijf implementeren. Een “standaard” firewall die voor iedereen werkt bestaat dus niet. In de volgende paragraaf wordt een overzicht gegeven van de security-wensen die firewalls kunnen vervullen.

Er zijn vele technieken beschikbaar waarmee de security-policy van een organisatie in de vorm van een firewall gerealiseerd kan worden: *IP-filtering*, *proxies*, *encryptie*, *virtual private networks (VPN)*, *email mapping*, *Network Address Translation (NAT)* en nog veel meer. De belangrijkste technieken worden verderop in dit white paper toegelicht.

In de volgende tabel wordt het verschil tussen security-policy en firewall-componenten, dus het verschil tussen doel en middel, toegelicht aan de hand van een aantal voorbeelden. De diverse termen in de tabel worden later toegelicht.

Doel	Techniek
Beperking van het verkeer van interne net naar Internet en vice-versa	IP-filters, proxies
Idem, met sterke authenticatie	challenge-response systemen, public-key certificaten
Gecontroleerd websurfen: bezoek aan bepaalde sites verboden en controle op de inhoud	screening proxy voor web-verkeer
Email: aparte interne en externe email-adressen controle op inhoud	screening conversie-tool anti-virus, anti-spyware
Interne IP-adressen onzichtbaar vanuit Internet	proxies NAT
Interne hostnamen onzichtbaar vanuit Internet	aparte interne en externe DNS-servers
Veilige koppeling met telewerkers en met andere bedrijven op Internet	Virtual Private Networks

Tabel 1: Security-doelen en security-technieken



2.2 Wat doet een firewall?

Een firewall heeft een uitgebreid takenpakket. Naast het reguleren van het verkeer tussen het interne netwerk en het Internet zijn er ook vele beheersmatige en administratieve taken. In de volgende paragrafen volgt een overzicht. Hierin wordt beschreven in welke termen de beveiligingswensen van een organisatie geformuleerd kunnen worden.

2.2.1 Reguleren van het verkeer

De centrale taak van een firewall is het reguleren van het verkeer tussen het interne netwerk en het Internet. Dit reguleren bestaat in hoofdzaak uit de volgende stappen:

- 1 Het in ontvangst nemen van een connectie-verzoek dat afkomstig is van een (interne of externe) client en gericht is aan een (externe of interne) server.
- 2 Het controleren of dit connectie-verzoek gehonoreerd mag worden.
- 3 Als dat het geval is: de connectie tussen client en server tot stand brengen.

Een firewall kan vele extra's bieden bij het vervullen van deze taak. Drie zeer belangrijke extra faciliteiten zijn:

- Het afdwingen van het gebruik van *sterke authenticatie* bij het opzetten van verbindingen. Sterke authenticatie wil zeggen dat een onweerlegbaar bewijs van identiteit geleverd wordt door een gebruiker of door een (client- of server-) programma. Authenticatie op basis van naam/wachtwoord combinaties of op basis van IP-adressen of domeinnamen wordt als *zwakke authenticatie* beschouwd: IP-adressen en domeinnamen kunnen door een technisch onderlegde aanvaller vervalst worden, terwijl namen en wachtwoorden afgeluisterd kunnen worden. Deze techniek is geschikt voor administratieve registratie (zoals registreren wie er browsed) maar is niet voldoende voor beveiligingstechnieken (zoals VPN en onderhoud). Sterke authenticatie kan plaatsvinden via cryptografische technieken zoals het gebruik van *public-key certificaten* of via *challenge-response* systemen zoals bijvoorbeeld girotel *one-time passwords* gebruikt (ook wel *tancode* lijsten genoemd) of zogenaamde *hand held authenticators* (*dongles*).



- Het bewaken van het protocol *na* het opbouwen van de verbinding en het controleren van de inhoud van de datastroom. Een voorbeeld van protocol bewaking is het toestaan van FTP download-operaties, maar verbieden van FTP upload-operaties (met als reden dat er geen informatie uit het bedrijfsnetwerk mag lekken). Een voorbeeld van inhoudscontrole is viruscontrole in mail en het toestaan van Websurfen en het verbieden van het gebruik van *Java applets* en *ActiveX controls* met het oog op de mogelijke security-problemen die deze met zich mee brengen.
- Logging van alle gebeurtenissen die betrekking hebben op de client-server verbinding: bijvoorbeeld het tijdstip waarop deze opgezet werd, de tijdsduur van de verbinding, de hoeveelheid getransporteerde bytes, de benaderde URL's, enzovoort.

2.2.2 Ondersteuning voor speciale toepassingen

Een aantal toepassingen is zo complex dat simpelweg doorlaten van het verkeer via de firewall niet voldoende is. Dit geldt met name voor de servers in het interne netwerk die vanuit het Internet benaderd moeten kunnen worden: email-servers, DNS servers en eventueel Web-servers.

Electronic mail

Electronic mail is een van de belangrijkste toepassingen van het Internet. Een veilige en probleemloze email-koppeling vergt de nodige maatregelen op de firewall. Mogelijke Email-diensten die een firewall kan verlenen zijn:

- Omdat de mail-server per definitie publiek toegankelijk is, zijn extra beveiligingsmaatregelen gewenst: Het verleden heeft uitgewezen dat complexe mail-server programmatuur erg inbraakgevoelig is. Extra bescherming is mogelijk door het gebruik van een *mail proxy* die binnenkomende post in eerste instantie ontvangt en deze controleert op “verdachte zaken” (zoals virussen en spyware). Alleen als deze controle positief uitvalt zal de post verwerkt worden.
- *Archivering* van elk passerend mailbericht (bijvoorbeeld in het kader van ISO 9000 procedures).
- *Maskerade*: het verbergen van interne machinenaamen in de afzenderadressen van uitgaande post.
- *Adres-vertalingen*: het door de firewall uitvoeren van vertaalslagen tussen intern in gebruik zijnde mailadressen en Internet-mailadressen. Dit kan vooral van pas komen in situaties waar er sprake is van fusies of reorganisaties waarbij de oude email adressen moeten blijven werken maar niet “naar buiten” mogen lekken, terwijl de nieuwe adressen al wel geaccepteerd worden.



- Het blokkeren of omleiden van ingaande en uitgaande post op basis van bepaalde criteria, zoals het afzender- of bestemmingsadres of attachmenttype, bijvoorbeeld in het kader van anti-virus, anti-spamming of anti-relay maatregelen.
- Het mogelijk maken om vanuit het Internet interne post te lezen, waarbij via encryptie en sterke authenticatie voor de vereiste beveiliging wordt gezorgd.

Websurfen

Na email is het surfen over het world wide web de meest populaire Internet toepassing. Net als bij email bevat het webverkeer soms gevaarlijke data zoals virussen en bevatten websites soms zaken zoals porno. Met een speciale www-proxy kan het verkeer gecontroleerd worden op correct gebruik van het HTTP protocol en ook op inhoud. Dergelijke proxies kunnen verkeer blokkeren naar bepaalde websites of voor bepaalde gebruikers.

DNS

Het Domain Name System (DNS) zorgt voor de vertalingen tussen hostnamen en IP-adressen. Daarnaast speelt DNS een rol bij het afleveren van elektronische post. Veel organisaties willen niet al hun interne hostnamen openbaar maken op het Internet. Hieraan kan worden voldaan door een firewall die een meervoudige DNS-functionaliteit biedt: bijvoorbeeld in de vorm van een externe name server die slechts enkele namen bekend maakt en vanuit het Internet is te bereiken en daarnaast een interne name server die alle namen bekend maakt en alleen vanuit het interne netwerk te bereiken is.

De Web-server

Vele organisaties bieden informatie over hun producten en diensten aan via een Web-server. Omdat deze meestal publiek toegankelijk is, zijn extra beveiligingsmaatregelen gewenst. Een voorbeeld van een dienst die de firewall kan bieden is het screenen van alle inkomende HTTP-verzoeken op verdachte zaken (content-attacks) en het op deze wijze beschermen van de Web-server. Daarnaast kan de firewall ook zorgen voor *load balancing*: het verdelen van de belasting over een aantal identieke exemplaren van de Web-server (ook wel “reverse-proxies” genoemd).

VPN (Tunneling en Virtual Private Networks)

Tunneling is een techniek waarbij twee netwerken met elkaar verbonden worden via het Internet. Een voorbeeld is het verbinden van twee Windows-netwerken via het Internet door de NetBios-pakketten in IP-pakketten in te pakken en over het Internet te versturen. Een ander voorbeeld is het verbinden van een mobiele- of thuiswerker met het bedrijfsnetwerk of van twee bedrijfsnetwerken via een *secure tunnel* die zorgt voor encryptie van alle dataverkeer. Men spreekt in dergelijke gevallen van een (*Secure*) *Virtual Private Network* (SVPN) of van een *Extranet*.



2.2.3 Beheersmatige taken van een firewall

Het is niet zo dat een eenmaal geïnstalleerde en werkende firewall geen verdere aandacht meer behoeft: er is een aantal permanent doorlopende beheersactiviteiten nodig. Dit is de reden dat security een *proces* is en geen product. Een overzicht volgt hieronder.

Logging en intrusion-detection

Logging is het registreren van een administratie met betrekking tot de netwerk- en andere activiteiten op de firewall. Logging is belangrijk vanuit security-oogpunt: aan een inbraak gaat vaak een periode vooraf waarin de inbreker probeert om binnen te komen. Als deze mislukte pogingen tijdig opgemerkt worden, kan men afdoende maatregelen treffen en zo een inbraak voorkomen. Daarnaast kan logging ook nuttig zijn in het kader van *accounting*: het doorbelasten van het gebruik van de firewall. Tenslotte is logging belangrijk bij het opsporen van misbruik uit de eigen organisatie.

Alerting

Een logging systeem voorziet ook in *alerting*, waarbij de firewall de beheerders direct attendeert op verdachte zaken in de logging.

System Integrity Checking / Intrusion Detection

System Integrity Checking is het regelmatig uitvoeren van “sanity checks” op de firewall, waarbij gecontroleerd wordt of essentiële processen nog steeds actief zijn, of er nog voldoende diskruimte vrij is en of er geen cruciale systeembestanden veranderd zijn (Host Intrusion Detection).

Aanpassingen in de configuratie

Van tijd tot tijd zullen aanpassingen in de configuratie van de firewall gewenst zijn.

Continuïteit

In elk systeem kan de rampspoed toeslaan in de vorm van hardware-problemen, spanningsuitval of andere onverwachte problemen die leiden tot onvoorspelbaar en dus onveilig gedrag. Tot de beheersaspecten van een firewall kunnen daarom ook zaken als *mirroring* en UPS support gerekend worden.

Actualiteit

Beveiliging is een onderwerp dat voortdurend in beweging is. Bugs in Web-, mail- en DNS-servers zorgen voor nieuwe gaten; nieuwe client-server protocollen brengen hun eigen specifieke security-problemen met zich mee en hackers ontdekken regelmatig nieuwe aanvalstechnieken. Bij een firewall hoort dan ook een constante stroom van patches, bug-fixes en technische vernieuwingen.



Ook hieruit blijkt dat security een voortdurend proces is.

2.2.4 Beveiliging van de firewall

Een firewall beveiligt het interne netwerk, maar dient ook zélf beveiligd te worden. Strikt noodzakelijke maatregelen zijn bijvoorbeeld:

- Processen, programma's en bestanden die voor het functioneren van het systeem niet nodig zijn, dienen van het systeem verwijderd te worden. Men noemt dit *hardening*.
- Functies in het besturingssysteem die niet nodig zijn dienen verwijderd te worden door een nieuw en gestript systeem te maken. Men noemt dit *stripping*.
- Toegang tot de firewall zelf dient beveiligd te worden door sterke authenticatie en encryptie. Een firewall waarop over het (interne) netwerk ingelogd kan worden via een naam/wachtwoord combinatie is kwetsbaar.

Uit het voorgaande volgt dat niet ieder systeem even geschikt is als platform voor een firewall. Voor een systeem dat zich gedraagt als een "black box" waar nauwelijks aan te sleutelen valt, zal het niet makkelijk zijn om een adequate *hardening* uit te voeren. UNIX systemen kunnen door hun hoge mate van flexibiliteit en configureerbaarheid wél vergaand gehardend en gestript worden. Daarom zijn veel firewalls gebaseerd op een meer of minder zichtbare UNIX kern.

2.2.5 Wat kan een firewall veelal niet?

In de voorgaande paragrafen is een reeks van taken genoemd die door een firewall kunnen worden uitgevoerd. Er zijn echter ook zaken die veel firewalls niet zonder meer kunnen beveiligen. Een van deze is het beschermen tegen een zogenaamde *content-attack*. Met *content-attack* wordt bedoeld dat via geoorloofde verbindingen gevaarlijke data het bedrijfsnetwerk in worden getransporteerd. Hierbij is het dus niet de connectie zelf die het probleem oplevert, maar de data die via die connectie getransporteerd wordt. Een voorbeeld is een PC-programma dat een virus bevat en dat met FTP of per email opgestuurd wordt. Maar steeds vaker worden firewalls geïntegreerd met speciale software voor virusdetectie en andere vormen van content-controle.

Een ander voorbeeld van een probleem dat de firewall niet makkelijk kan detecteren is een uitgaand email-bericht waarin vertrouwelijke bedrijfsgegevens verstuurd worden. Ook op dit gebied zien we recentelijk interessante ontwikkelingen: sommige firewalls proberen het ongewenst uitlekken van bedrijfskritische informatie te detecteren door te controleren op de aanwezigheid van specifieke trefwoorden in uitgaande email-berichten en bestanden. Overigens kan de firewall ook altijd een archief van inkomende en uitgaande email-berichten aanleggen, zodat dit soort zaken achteraf vastgesteld kan worden.

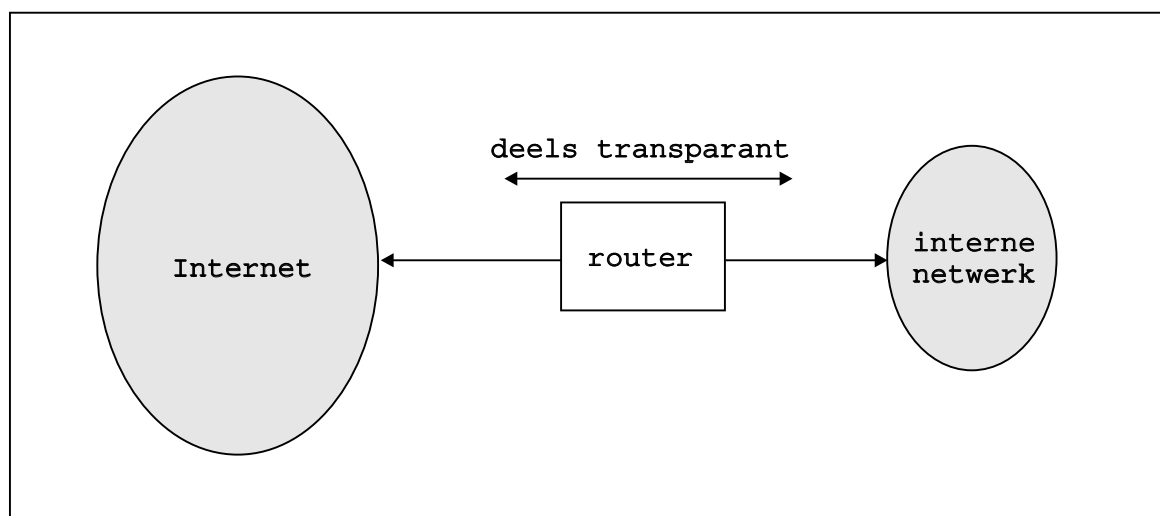


2.3 Hoe werkt een firewall?

In de nu volgende paragrafen geven we een overzicht van enkele veel toegepaste firewall-technieken. We benadrukken nogmaals dat de te gebruiken mix van technieken in elke situatie weer opnieuw bepaald moet worden, na het in kaart brengen van de security-policy.

2.3.1 IP-filters

Een zeer veel toegepaste beveiligingstechniek is IP-filtering. Een IP-filter inspecteert binnenkomende pakketten en laat ze door op basis van een aantal filter-criteria. De belangrijkste criteria zijn het gebruikte protocol (bijvoorbeeld TCP of UDP), het IP-adres van de afzender en de bestemming van het pakket en het poortnummer van de gebruikte toepassing (bijvoorbeeld TELNET, FTP, HTTP of SMTP).



Figuur 1: IP-filtering

De bekendste voorbeelden van IP-filteraars zijn routers. Er is echter ook speciale software waarmee een UNIX- of Windows-systeem met meerdere netwerk-interfaces als IP-filteraar kan optreden.

Voorbeelden van security-maatregelen die door configuratie van een IP-filter gerealiseerd kunnen worden, zijn:



- Een IP-filter als *diode*: machines op het lokale netwerk mogen contact zoeken met het Internet, maar het omgekeerde is niet toegestaan. Een voorbeeld is de situatie waarin uitgaand telnet-verkeer is toegestaan, maar inkomend telnet-verkeer verboden wordt. Voor sommige protocollen, zoals FTP en Realaudio, is een diode geen goede oplossing omdat er sprake is van een (extra) connectie die op initiatief van de server wordt opgezet.
- Een IP-filter als *selectief filter*: bepaalde machines op het lokale netwerk mogen contact zoeken met bepaalde machines op het Internet en bepaalde machines op het Internet mogen contact zoeken met bepaalde machines in het lokale netwerk.
Het is ook mogelijk om hierbij restricties te stellen aan de gebruikte programma's: bijvoorbeeld van buiten naar binnen mag vanaf bepaalde machines contact gezocht worden, maar alleen met *bepaalde servers*, bijvoorbeeld alleen met de telnet-server en de FTP-server.

De voor- en nadelen van een IP-filter als firewall-techniek zijn als volgt samen te vatten:

- Een voordeel is dat het gebruik van een IP-filter voor de gebruiker en de applicatiesoftware geheel transparant is: aanpassingen zijn niet nodig. Omdat een IP-filter weinig filterwerk hoeft te verrichten is de performance hoger dan van een vergelijkbare proxy-firewall.
- Een nadeel is dat niet aan autorisatie van *gebruikers* wordt gedaan: deze ligt geheel aan de bestemmingszijde, bijvoorbeeld op de bestemmingsmachine in het interne netwerk. Vandaar dat bij gebruik van een IP-filter de machines in het interne netwerk die als bestemming mogen optreden, zeer zorgvuldig gekozen en beheerd moeten worden.
- Het schrijven van foutloze filter-tabellen is niet eenvoudig: de syntax is lastig en foutcontrole is moeilijk. Constateren dat het IP-filter een verbinding toestaat is eenvoudig, maar controleren of het alle verboden verbindingen daadwerkelijk weigert is een stuk moeilijker.
- Het filteren op basis van informatie in het netwerkpakket zit vol voetangels en klemmen. Zo is controle op de *geldigheid* van een afzender-adres van een netwerkpakket niet mogelijk: een afzender op het Internet kan een oneigenlijk adres gebruiken (*adres spoofing*).
- IP-filters laten pakketten door als de inspectie positief uitvalt. Een doorgelaten IP-pakket kan echter best nog kwalijke IP- of TCP-header componenten bevatten die schade kunnen aanrichten aan systemen in het interne netwerk. Een voorbeeld vormen *denial of service* aanvallen met behulp van gemanipuleerde IP- of TCP-headers. Op proxies gebaseerde beveiliging voorkomt dit probleem.
- IP-filters hebben geen kennis op applicatie-niveau. Beperkingen op applicatie-niveau, zoals virus-checking voor inkomende mailberichten, het toestaan van Websurfen maar filteren van Java en ActiveX en het blokkeren van inkomende HTTP PUT-operaties kennen IP-filters niet. Pakketten die doorgelaten worden door een IP-filter kunnen daarom mogelijkwijs wel degelijk schade aanrichten.



- IP-filters bevatten meestal geringe *logging*-faciliteiten: uitgebreide mogelijkheden om speciale gebeurtenissen in logfiles weg te schrijven ontbreken vrijwel altijd.

Conclusie: een IP-filter is weliswaar een nuttig onderdeel van een firewall, maar biedt op zichzelf nooit afdoende bescherming.

2.3.2 Stateful Inspection

Een verbeterde vorm van IP-filtering, waarmee een deel van de tekortkomingen van een pure IP-filter firewall kan worden opgelost, wordt verkregen door het IP-filter uit te rusten met een inspection-engine die kennis heeft van de sessies die zijn opgestart. Dit wordt *Stateful Inspection* genoemd.

In zijn tabellen houdt een Stateful Inspection filter, op basis van source/destination/protocol/poort, bij welke sessies zijn opgezet. Tevens kijkt het filter, afhankelijk van de state, of het antwoord bij een bepaalde vraag hoort en of het antwoord legitiem is. Een dergelijke controle kan op meerdere netwerk-niveau's plaatsvinden (multi-layer). Onder meer wordt geïnspecteerd:

- Communicatie informatie
- Status van de communicatie (tracering van commando's)
- Status van de applicatie
- Manipulatie van informatie

De stateful inspection firewall kent een aantal voor- en nadelen:

- Behoorlijk beveiligingsniveau met behoud van performance
- (Beperkt) inzicht in applicatie-verkeer
- Transparantie
- Beveiligingsniveau is niet het hoogst haalbare
- Als een Stateful Inspection firewall faalt, kunnen er zwakke plekken ontstaan in de beveiliging omdat er geen sprake is van gelaagde beveiliging (defense in depth).

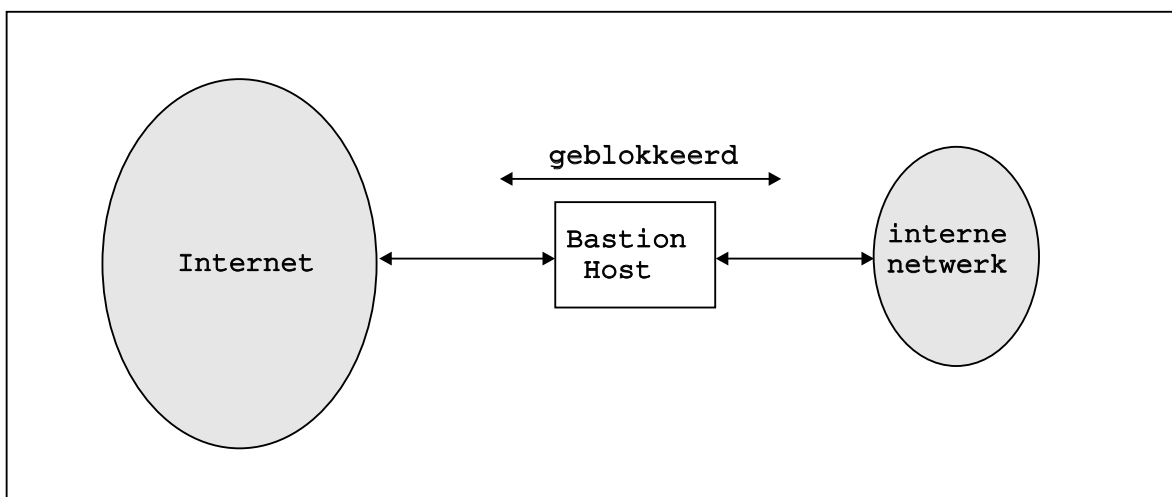


2.3.3 Proxies

Een proxy is een proces dat een tussenstap tussen de client en de server vormt. Hieronder wordt een onderscheid gemaakt tussen *gewone proxies*, de *connectie-level proxies* en *transparante proxies*. Het kenmerk van een firewall die met proxies werkt is in alle gevallen dat er nooit IP-pakketten uit het Internet op het interne net komen en dat er dus ook geen aanval op TCP- of IP-niveau (zoals bijvoorbeeld de Ping of death of teardrop aanval) uitgevoerd kan worden.

2.3.3.1 Proxies

De werkwijze bij het gebruik van een gewone proxy is als volgt:



Figuur 2: Het gebruik van een proxy

- 1 Gebruikers die een bepaalde dienst willen benaderen, moeten zich eerst melden bij de proxy-server op de firewall.
- 2 De proxy bepaalt of het verzoek van de gebruiker gehonoreerd mag worden. Een Web-proxy kan het recht op Websurfen bijvoorbeeld voorbehouden aan specifieke interne gebruikers die dat voor hun werk nodig hebben. In zijn algemeenheid kan de authenticatie van gebruikers door een proxy plaatsvinden op basis van het IP-adres of de domeinnaam, op basis van een naam/wachtwoord combinatie of op basis van sterkere technieken zoals challenge-response systemen of public-key certificaten. De feitelijk beschikbare authenticatie-technieken kunnen per proxy verschillend zijn en hangen dus af van de proxy-software.

- 3 Daarna bouwt de proxy-server een verbinding op met de “echte” server. Er bestaat dus geen IP-verbinding tussen client en server: in plaats daarvan zijn er aparte verbindingen tussen de client en de proxy-server en tussen de proxy-server en de “echte” server.
- 4 Afhankelijk van het soort proxy zal deze de communicatie tussen de client en de server al dan niet verder bewaken. Een Web-proxy zou toegang tot bepaalde sites (black-listing) of het gebruik van Java en ActiveX kunnen verbieden, terwijl een FTP-proxy bepaalde FTP-commando's kan blokkeren.

Het is belangrijk om op te merken dat een proxy een doorgeefluik vormt voor één bepaalde applicatie. Dat heeft voor- en nadelen:

- Het grote voordeel is dat de proxy kennis heeft van de applicatie en daarom desgewenst ook voor applicatie-specifieke beveiligingsmaatregelen kan zorgen. Dit wordt *protocol screening* genoemd. Voorbeelden van protocol screening werden hierboven reeds gegeven: het tegenhouden van ftp-uploads, of van het gebruik van Java-applets in Web-pagina's en het detecteren van virussen in mail- of webverkeer.
- De prijs voor de applicatie-specifieke kennis van een proxy is dat er per applicatie een aparte proxy nodig is. Dit is een duidelijk nadeel ten opzichte van een IP-filter, dat voor alle applicaties bruikbaar is.
- Een ander nadeel is dat ófwel de client ófwel (het gedrag van) de gebruiker moet worden aangepast: er moet immers een tussenstap op de proxy worden gemaakt.

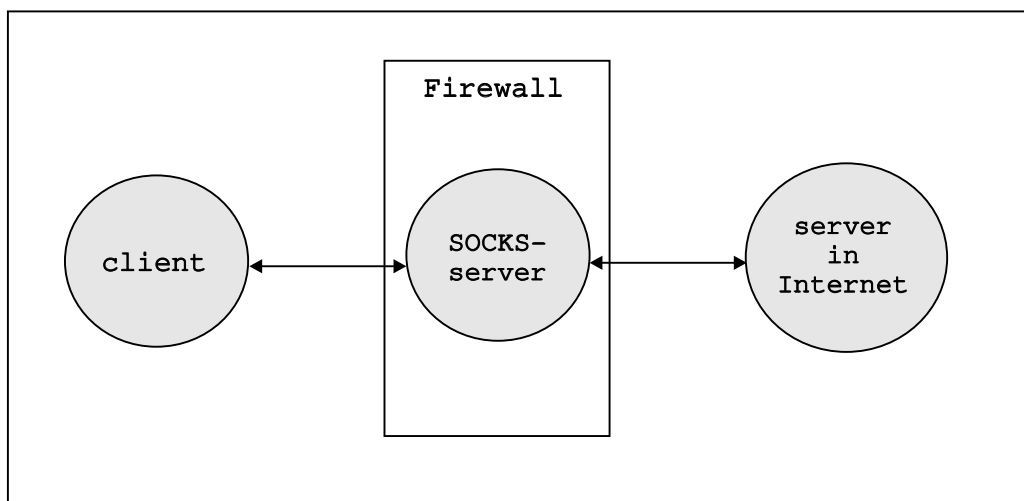
Voor de meeste belangrijke toepassingen zijn proxies beschikbaar. Dat geldt bijvoorbeeld voor SMTP, HTTP, FTP, HTTPS, SSL, rsh, telnet, RealAudio en X11.



2.3.3.2 Connectie-level proxies

Een nadeel van gewone proxies is dat er per applicatie een aparte proxy nodig is. Er is echter een soort “generieke” proxy ontwikkeld, die in principe voor elke applicatie (mits deze op het TCP protocol is gebouwd) te gebruiken is. De software die hiervoor gebruikt wordt staat bekend onder de naam SOCKS (socks protocol versie 4).

Bij gebruik van SOCKS vinden de volgende stappen plaats:



Figuur 3: Het gebruik van SOCKS

- 1 Wanneer een client een server (bijvoorbeeld in het Internet) wil benaderen, moet hij met dit verzoek aankloppen bij de SOCKS-server op de firewall.
- 2 De SOCKS-server bepaalt op basis van een aantal criteria (o.a. het IP-adres van de client en de gebruikersnaam) of toegang tot het Internet is toegestaan voor de client en de gebruiker in kwestie. Zo ja, dan zal de SOCKS-server het client-verzoek doorspelen aan de “echte” server.
- 3 Het antwoord van de server komt in eerste instantie binnen bij de SOCKS-server.
- 4 De SOCKS-server geeft het antwoord door aan de client.

Het voordeel van SOCKS is dat het voor de meeste (TCP-) applicaties te gebruiken is. Er zijn echter ook nadelen:



- Uit het voorgaande blijkt dat voor gebruik van SOCKS aanpassingen in de client-software noodzakelijk zijn.
- In tegenstelling tot de gewone proxies heeft SOCKS geen kennis van de applicaties zelf, zodat beveiliging op applicatieniveau (bijvoorbeeld niet naar buiten toe kopiëren bij FTP) niet mogelijk is. SOCKS speelt zich af op het *connectie-niveau*: het biedt beveiliging op het niveau van de (TCP-)connectie, niet op het niveau van de applicatie.
- Een derde nadeel is dat er bij gebruik van SOCKS geen faciliteiten voor sterke authenticatie zijn.

In de praktijk wordt soms een combinatie van SOCKS met gewone proxies gebruikt: de firewall kan bijvoorbeeld voorzien worden van gewone proxies voor FTP en telnet en daarnaast van de SOCKS software voor overige TCP-toepassingen.

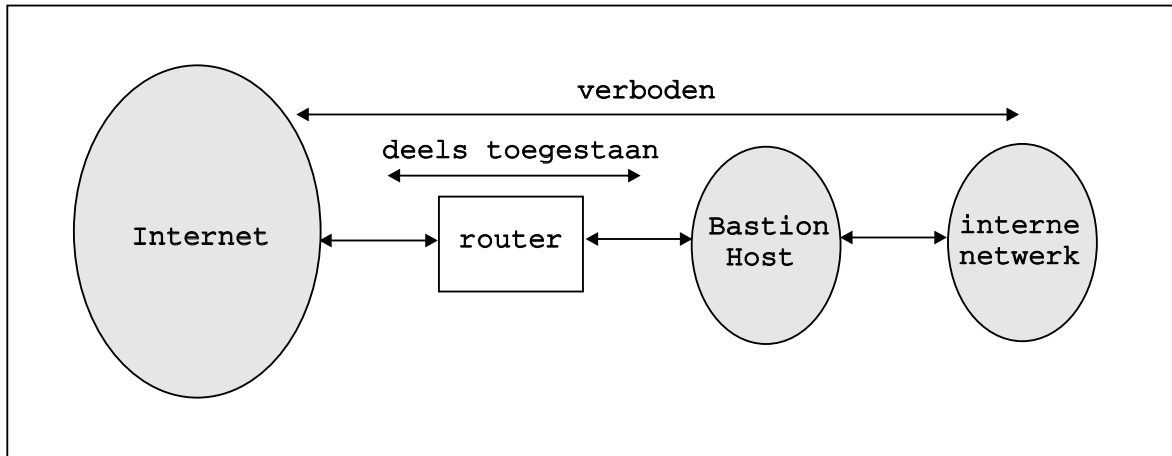
2.3.3.3 Transparante proxies

Een belangrijk nadeel van de gewone proxies is dat ze niet transparant zijn: de client of gebruiker moet erop geprepareerd worden om een tussenstap op de proxy te maken. Bij gebruik van een *transparante proxy* is dat niet nodig: de client kan de gewenste server rechtstreeks benaderen - althans dat lijkt zo voor de client. Door speciale aanpassingen in de firewall zal deze poging tot verbindingsopbouw onderschept worden en zal de juiste proxy automatisch worden gestart. Deze proxy bouwt dan een verbinding op naar de aangegeven server. De client hoeft niet speciaal te worden geconfigureerd om een verbinding met de proxy te maken maar lijkt rechtstreeks verbinding met de server te hebben. De op deze wijze automatisch geactiveerde proxy kan zich vervolgens als een applicatie-bewuste proxy gedragen of als een applicatie-onafhankelijke proxy. In het eerste geval zal de aanwezigheid van de proxy overigens niet altijd transparant blijven voor de gebruiker: deze kan geconfronteerd worden met eventuele door de proxy opgelegde beperkingen.

2.3.4 Een screened bastion host

Een veelgebruikte architectuur voor een firewall is een *screened bastion host* en IP-filters. Dit is een combinatie van een router en een UNIX- of Windows-systeem waarop proxies geïnstalleerd zijn. Op deze wijze worden de voordelen van deze beide technieken gecombineerd. De router wordt bovendien zodanig geconfigureerd dat hij alleen verkeer toestaat tussen de bastion host en het Internet.





Figuur 4: Een screened bastion host als firewall

Er zijn vele variaties mogelijk op deze topologie. De bastion host kan bijvoorbeeld één of meerdere netwerk-interfaces hebben of in een apart subnet opgenomen worden. De te kiezen variant hangt af van de specifieke beveiligings- en functionaliteitswensen.

2.3.5 Poort en Network Address Translation (PAT en NAT)

Poort en Network Address Translation is een techniek waarbij de firewall een vertaalslag uitvoert op IP-adressen en gebruikte poortnummers. Bij gebruik van proxies is PAT en NAT in feite impliciet, omdat de proxy een nieuwe connectie met de buitenwereld zal opzetten. Daarnaast bieden de meeste firewalls ook PAT en NAT-faciliteiten op IP-niveau.

Address Translation kan worden toegepast om interne adressen onzichtbaar te maken vanuit het Internet. Er zijn verschillende redenen waarom dat gewenst kan zijn:

- Uit veiligheidsoverwegingen: om inzicht in de structuur van het interne netwerk te verhinderen.
- Omdat in het interne netwerk de speciale IP-adressen voor *private Internets* worden gebruikt (zie onder meer RFC 1918: "Address Allocation for Private Internets").
- Omdat intern IP-adressen gebruikt worden die officieel van een andere organisatie zijn. Voor dit specifieke geval is moeilijk een oplossing te vinden: de meeste firewall-oplossingen kunnen de externe organisaties waarvan de misbruikte adresruimte eigenlijk is niet bereiken (omdat deze de betreffende adressen met interne hosts associeert).

2.3.6 SPAM detectie- en filtering-technieken

Recentelijk wordt een grote toename van ongevraagde (reclame) email (die in het algemeen wordt aangeduid als SPAM) gesignaleerd. Met het blokkeren van SPAM blijkt in de praktijk niet alleen een aanzienlijke besparing van Internet-bandbreedte te worden gerealiseerd, maar het bespaart dagelijks ook al snel 10 á 20 minuten afhandelingstijd *per email-gebruiker*. Blokkerende maatregelen die de enorme toename aan ongevraagde (meestal commerciële) boodschappen indammen, dragen daarom bij aan de productiviteit.

Er zijn twee methoden om SPAM geautomatiseerd te herkennen:

- 1 Met de eerste methode wordt, nog voordat de email daadwerkelijk is aangenomen, gecontroleerd aan de hand van de afzender of deze bekend staat als een *spammer*. Als dat zo is dan wordt de email geweigerd. Deze methode is erg effectief omdat de mail niet eens over de Internet-verbinding hoeft voordat ze wordt afwezen.
- 2 Met de tweede methode wordt de inhoud van een email bekeken. Op basis van herkenbare woorden of slimmere herkennings-algoritmen volgt een uitspraak over de kans dat deze email inderdaad SPAM is. Vergeleken met de eerste methode is deze methode effectiever om SPAM te *herkennen*.

Beide systemen worden in de volgende paragrafen in meer detail beschreven.

2.3.6.1 Methode 1: afzender-controle

De *afzender* van een email kan op twee manieren worden bepaald:

- a Via het afzender IP-adres. Bij deze methode kan meteen na het maken van de netwerkverbinding het afzender-IP-adres worden opgezocht in een database. Als het adres in de database voorkomt, dan wordt een foutmelding gestuurd (om het opnieuw zenden van de boodschap te voorkomen) en de verbinding wordt gesloten. De netwerkbelasting is bij deze methode minimaal.
- b Via het afzender email-adres. Het adres dat in het bericht staat wordt opgezocht in een database. Als het adres in de database voorkomt dan wordt een foutmelding gestuurd (om het herzenden van de boodschap te voorkomen) en de verbinding wordt gesloten. De netwerkbelasting is ook bij deze methode minimaal.

De tweede methode (b) is niet zo populair omdat SPAM-verzenders veelal willekeurige afzender-namen gebruiken. De eerste methode is erg effectief maar de kwaliteit van de database is belangrijk: een database waarin vervuiling voorkomt, zorgt voor onterechte blokkades (false positives). Er zijn drie typen databases:



- 1 Databases die de beheerder van een organisatie zelf bijhoudt. Deze databases zijn zeer bewerkelijk en doorgaans niet erg effectief omdat geen gebruik gemaakt wordt van de wereldwijde (collectieve) kennis van SPAM-adressen.
- 2 Databases van non-profit organisaties zoals b.v. Spamcop. Deze maken wel gebruik van de wereldwijde (collectieve) kennis van SPAM-adressen maar bevatten relatief veel vervuiling en geven geen garantie op beschikbaarheid.
- 3 Databases van commerciële organisaties zoals b.v. RBL+. Deze maken gebruik van de wereldwijde (collectieve) kennis van SPAM-adressen, bevatten weinig vervuiling (de toe te voegen adressen worden beter gecontroleerd) en geven wel garantie op beschikbaarheid.

2.3.6.2 Methode 2: inhoudscontrole

Het controleren van de inhoud van een email kan op allerlei manieren gebeuren. Het voert te ver om deze methoden te bespreken maar alle methoden hebben drie gemeenschappelijke kenmerken:

- De inhoudscontrole doet een uitspraak over de *kans* dat een boodschap SPAM is.
- Spammers zullen hun boodschappen steeds anders verpakken om de herkenningsalgoritmen te omzeilen. Daarom is er, net als bij afzender-controle, een update-faciliteit nodig (b.v. in de vorm van een abonnement, zoals bij een virus scanner) om de herkenningsalgoritmen up to date te houden.

