Linux Network Server: Firewalls

Dr. A.R. (Tom) Peters
HvA/HI
gastdocent
Hogeschool van Amsterdam, afd. Hogere Informatica

tpeters@xs4all.nl
0204080204

Leerdoelen Firewalls

Wees in staat om de betekenis en functie uit te leggen van het begrip *"firewall"* en gerelateerde begrippen, en hun onderlinge samenhang; met name:

- IP packet filtering
- IP masquerading
- tcpwrappers
- proxies

0. Firewalls

1. Firewall

Uit RFC2828: "Internet Security Glossary" (http://www.rfc-editor.org/rfc/rfc2828.txt) :

```
firewall
      (I) An internetwork gateway that restricts data communication
      traffic to and from one of the connected networks (the one said to
```

be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). (See: guard, security gateway.)

(C) A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies security policy rules to control traffic that flows in and out of the protected network.

(C) A firewall is not always a single computer. For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN between the two routers. The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers. The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep intruders out, but usually also needs to let authorized users in and out.

2. Gateway

Uit RFC2828: "Internet Security Glossary" (http://www.rfc-editor.org/rfc/rfc2828.txt) :

```
$ gateway
      (I) A relay mechanism that attaches to two (or more) computer
      networks that have similar functions but dissimilar
```

```
      implementations and that enables host computers on one net-
work to
      communicate with hosts on the other; an intermediate system that
      is the interface between two computer networks. (See: bridge,
      firewall, guard, internetwork, proxy server, router, and
      subnetwork.)

      (C) In theory, gateways are conceivable at any OSI layer. In
      practice, they operate at OSI layer 3 (see: bridge, router) or
      layer 7 (see: proxy server). When the two networks differ in the
      protocol by which they offer service to hosts, the gateway may
      translate one protocol into another or otherwise facilitate
      interoperation of hosts (see: Internet Protocol).
```

3. Proxy

Uit RFC2828: "Internet Security Glossary" (http://www.rfc-editor.org/rfc/rfc2828.txt) :

```
proxy server
      (I) A computer process--often used as, or as part of, a firewall-
-
      that relays a protocol between client and server computer systems,
      by appearing to the client to be the server and appearing to the
      server to be the client. (See: SOCKS.)

      (C) In a firewall, a proxy server usually runs on a bastion host,
      which may support proxies for several protocols (e.g., FTP, HTTP,
      and TELNET). Instead of a client in the protected enclave
      connecting directly to an external server, the internal client
      connects to the proxy server which in turn connects to the
      external server. The proxy server waits for a request from inside
      the firewall, forwards the request to the remote server outside
      the firewall, gets the response, then sends the response back to
      the client. The proxy may be transparent to the clients, or they
```

```
      may need to connect first to the proxy server, and then use that
      association to also initiate a connection to the real server.

      (C) Proxies are generally preferred over SOCKS for their ability
      to perform caching, high-level logging, and access control. A
      proxy can provide security service beyond that which is normally
      part of the relayed protocol, such as access control based on peer
      entity authentication of clients, or peer entity authentica-
tion of
      servers when clients do not have that capability. A proxy at OSI
      layer 7 can also provide finer-grained security service than can a
      filtering router at OSI layer 3. For example, an FTP proxy could
      permit transfers out of, but not into, a protected network.
```

4. Overige Begrippen

- bastion host
- guard
- security gateway
- SOCKS

5. Security in TCP/IP Stack

Figure 1. Security in TCP/IP stack

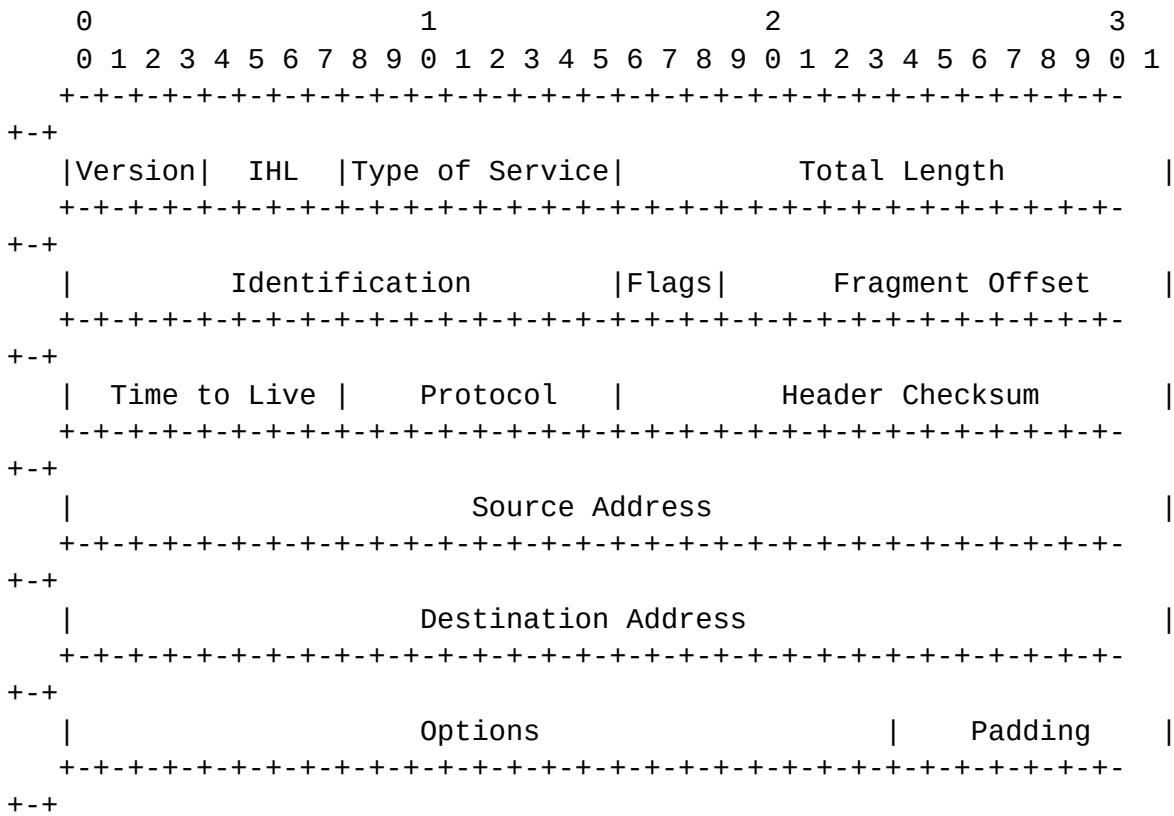
Veiligheidsmaatregelen (voor firewalls) in verschillende network layers.

6. Filtering

- *IP layer*: packet filtering; snel, dom.
- *TCP layer*: packet filtering, port forwarding; snel, selectief, logging.
- *Application layer*: proxies; traag, selectief, caching, logging, authenticatie.

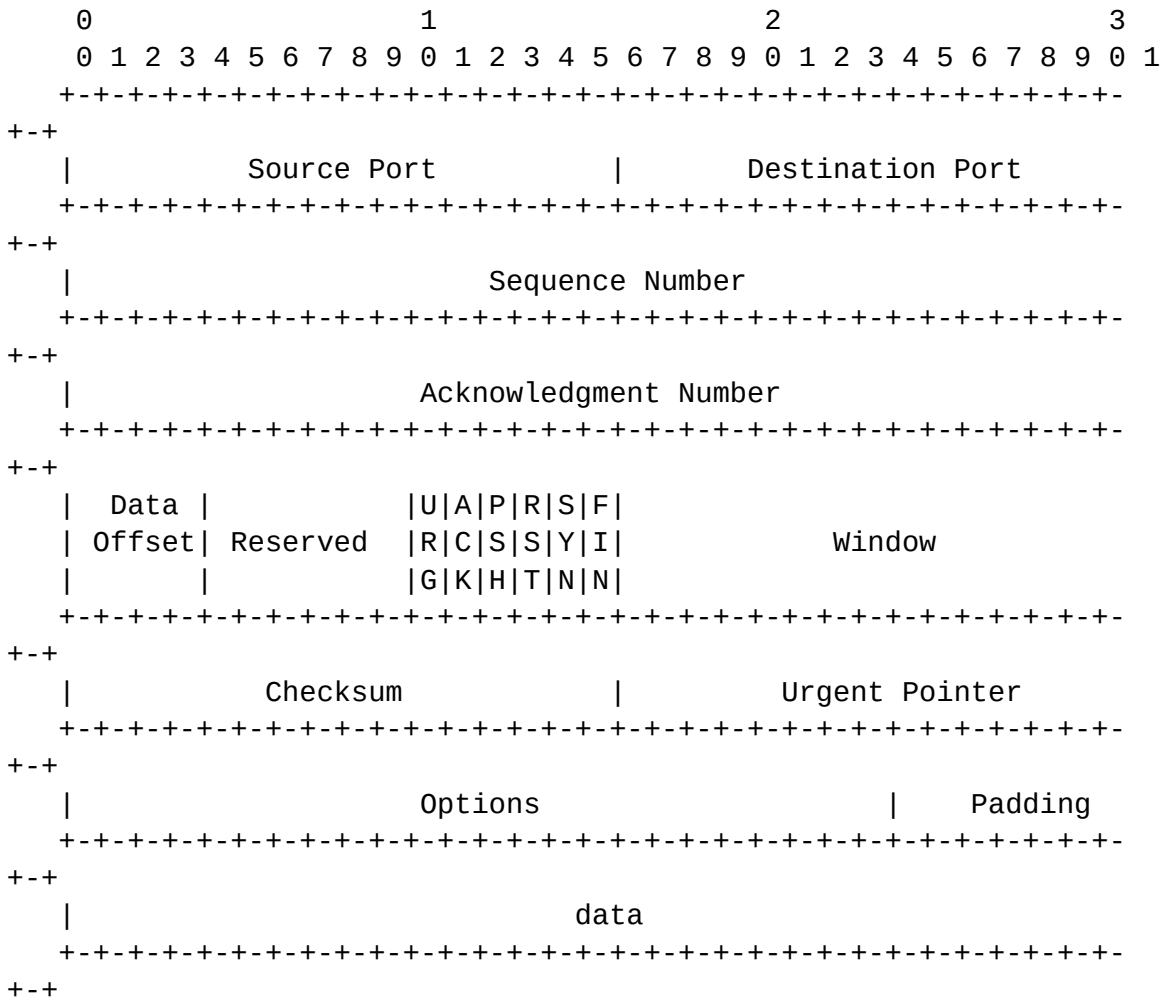
7. IP Packets

IP header: bytes 1..20 of ..24 ; uit RFC791: "Internet Protocol" (http://www.rfc-editor.org/rfc/rfc791.txt) .



8. TCP Packets

TCP header: na IP header, bytes 21..40 of ..44 ; uit RFC793: "Transmission Control Protocol" (http://www.rfc-editor.org/rfc/rfc793.txt) .



9. Linux Filtering

- Packet Filtering op IP adres en TCP port, masquerading, port forwarding.
  - *Network Address Translation = masquerading*, eigenlijk een zaak van *routing*:

    ```
    Intranet adres  --> Firewall  --> Internet
                    <--           <--
    ```

  - *Port Forwarding*:

    ```
    Intranet port service <--  Firewall <-- Internet vraagt port ser-
    vice
                           -->
    ```

  - Kernel 2.0.x: **ipfwadm**
  - Kernel 2.2.x: IPChains: **ipchains**; **ipmasqadm**
  - Kernel 2.4.x: Netfilter: **iptables**

- Monitoring op TCP port: TCP wrappers
- Per applicatie (TCP service): proxy servers

10. IPChains

Aanbevolen literatuur:

- http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html

- http://www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO.html
- http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html
- Jeff Regan: "An Introduction to Using Linux as a Multipurpose Firewall". Linux Journal 71, Mar. 2000, "Strictly On-Line" (http://noframes.linuxjournal.com/lj-issues/issue71/3546.html)
- Preston F. Crow: "The Linux Home Network". Linux Journal 72, Apr. 2000, pp.80..84 (http://noframes.linuxjournal.com/lj-issues/issue72/3575.html)
- Jan Stumpel: "A Private Home Network". Linux Gazette 65, April 2001 (http://www.linuxgazette.org/issue65/stumpel.html)

11. Netfilter

Aanbevolen literatuur:

- *Packet Filtering* (iptables): http://netfilter.filewatcher.org/unreliable-guides/packet-filtering-HOWTO/index.html
- *Network Address Translation*: http://netfilter.filewatcher.org/unreliable-guides/NAT-HOWTO/index.html
- Zie ook: http://www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO-2.html#ss2.7

12. TCP Wrappers

-

  `inetd (8) - internet super-server`

  - beheert alle TCP ports

- start per port een programma, bijv. een server
- configuratie in `/etc/inetd.conf`

- TCP wrappers:
  - `tcpd (8) - access control facility for internet services`
  - wordt gestart door **inetd**, met uiteindelijke *port server* als parameter (volgens `/etc/inetd.conf`)
  - beslist over starten van de *port server* volgens `/etc/hosts.deny` en `/etc/hosts.allow`
  - Zie:
    `hosts_access (5) - format of host access control files`
  - logging via **syslogd** volgens `/etc/syslog.conf`

13. Remote Procedure Calls

Remote Procedure Call:

- verouderde methode voor *remote access* van Sun
- nog gebruikt voor *Network File System* (NFS) en *Network Information System* (NIS, NIS+)
- run **portmap** om te vertalen tussen RPC's en TCP ports:
  `portmap (8) - DARPA port to RPC program number mapper`
- **rsh** en **rcp** vervangen door **ssh** en **scp** !

14. Proxies

- **squid**:
  - voor HTTP
  - ook *caching*

- SOCKS:
  - generieke proxy
  - alleen TCP, geen UDP
  - RFC1928: SOCKS Protocol V.5 (http://www.rfc-editor.org/rfc/rfc1928.txt)
  - schijnt verouderd te zijn (geen "echte" proxy)

16. Literatuur

16.1. The Linux Documentation Project:

http://www.linuxdoc.org/

- http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html
- http://www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO.html

  Zie ook Linux IP Masquerade Resource: http://ipmasq.cjb.net/

- http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html

- Zie ook TrinityOS:
  http://www.ecst.csuchico.edu/~dranch/LINUX/TrinityOS/cHTML/TrinityOS-c.html

16.2. Netfilter (Kernel 2.4):

http://netfilter.filewatcher.org/

- Packet Filtering (iptables):
  http://netfilter.filewatcher.org/unreliable-guides/packet-filtering-HOWTO/index.html
- Network Address Translation:
  http://netfilter.filewatcher.org/unreliable-guides/NAT-HOWTO/index.html

16.3. RFC's:

- RFC791: Internet Protocol (http://www.rfc-editor.org/rfc/rfc791.txt)
- RFC793: Transmission Control Protocol (http://www.rfc-editor.org/rfc/rfc793.txt)
- RFC1700: Assigned Numbers (http://www.rfc-editor.org/rfc/rfc1700.txt)

  Voor *up-to date Assigned Numbers*, zie: http://www.iana.org/numbers.htm

  Voor TCP port numbers, zie ook:
  ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers

- RFC1928: SOCKS Protocol V.5 (http://www.rfc-editor.org/rfc/rfc1928.txt)

16.4. Linux Journal & Linux Gazette:

- Jeff Regan: "An Introduction to Using Linux as a Multipurpose Firewall". Linux

Journal 71, Mar. 2000, "Strictly On-Line" (http://noframes.linuxjournal.com/lj-issues/issue71/3546.html)

- Preston F. Crow: "The Linux Home Network". Linux Journal 72, Apr. 2000, pp.80..84 (http://noframes.linuxjournal.com/lj-issues/issue72/3575.html)
- Lawrence Teo: "Setting up a Linux Gateway". Linux Journal 72, Apr. 2000, pp.86..88
- Marcel Gagné: "A Few Recipes for Easier Firewalls". Linux Journal 78, Oct. 2000, pp.40..46 (http://noframes.linuxjournal.com/lj-issues/issue78/4218.html)
- Jan Stumpel: "A Private Home Network". Linux Gazette 65, April 2001 (http://www.linuxgazette.org/issue65/stumpel.html)

17. Huiswerk

Zoek uit wat voor soort firewall, NAT, proxy services, en andere services er nodig zijn voor dit project. Maak hiervoor gebruik van de relevante literatuur, m.n.:

- http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html
- http://www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO.html

  Zie ook Linux IP Masquerade Resource: http://ipmasq.cjb.net/

- http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html
- TrinityOS: http://www.ecst.csuchico.edu/~dranch/LINUX/TrinityOS/cHTML/TrinityOS-c.html