Firewall (networking)

From Wikipedia, the free encyclopedia

In computing, a **firewall** is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction. A firewall is also called a **Border Protection Device** (**BPD**), especially in NATO contexts, or **packet filter** in BSD contexts. A firewall has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

Proper configuration of firewalls demands skill from the administrator. It requires considerable understanding of network protocols and of computer security. Small mistakes can render a firewall worthless as a security tool.

Contents

Types of firewalls

There are three basic types of firewalls depending on:

- Whether the communication is being done between a single node and the network, or between two or more networks.
- Whether the communication is intercepted at the network layer, or at the application layer.
- Whether the communication state is being tracked at the firewall or not.

With regard to the scope of filtered communications there exist:

- Personal firewalls, a software application which normally filters traffic entering or leaving a single computer.
- Network firewalls, normally running on a dedicated network device or computer positioned on the boundary of two or more networks or DMZs (demilitarized zones). Such a firewall filters all traffic entering or leaving the connected networks.

The latter definition corresponds to the conventional, traditional meaning of "firewall" in networking.

In reference to the layers where the traffic can be intercepted, three main categories of firewalls exist:

- Network layer firewalls. An example would be iptables.
- Application layer firewalls. An example would be TCP Wrapper.
- Application firewalls. An example would be restricting ftp services through /etc/ftpaccess file

These network-layer and application-layer types of firewall may overlap, even though the personal firewall does not serve a network; indeed, single systems have implemented both together.

There's also the notion of application firewalls which are sometimes used during wide area network (WAN) networking on the world-wide web and govern the system software. An extended description would place them lower than application layer firewalls, indeed at the Operating System layer, and could alternately be called operating system firewalls. Some firewalls have higher privileges than others like mysql and pj.

Lastly, depending on whether the firewalls track packet states, two additional categories of firewalls exist:

- Stateful firewalls
- Stateless firewalls

Network layer firewalls

Main article: network layer firewall

Network layer firewalls operate at a (relatively) low level of the TCP/IP protocol stack as IP-packet filters, not allowing packets to pass through the firewall unless they match the rules. The firewall administrator may define the rules; or default built-in rules may apply (as in some inflexible firewall systems).

A more permissive setup could allow any packet to pass the filter as long as it does not match one or more "negative-rules", or "deny rules". Today network firewalls are built into most computer operating systems and network appliances.

Modern firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, domain name of the source, and many other attributes.

Application-layer firewalls

Main article: application layer firewall

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgement to the sender). In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines.

By inspecting all packets for improper content, firewalls can even prevent the spread of the likes of viruses. In practice, however, this becomes so complex and so difficult to attempt (given the variety of applications and the diversity of content each may allow in its packet traffic) that comprehensive firewall design does not generally attempt this approach.

The XML firewall exemplifies a more recent kind of application-layer firewall.

Proxies

Main article: Proxy server

A proxy device (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, whilst blocking other packets.

Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly-reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as *IP spoofing* to attempt to pass packets to a target network.

Network address translation

Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly use so-called "private address space", as defined in RFC 1918. Administrators often set up such scenarios in an effort (of debatable effectiveness) to disguise the internal address or network.

Management

The Middlebox Communication (midcom) Working Group of the Internet Engineering Task Force is working on standardizing protocols for managing firewalls and other middleboxes. See, e.g., Middlebox Communications (MIDCOM) Protocol Semantics (ftp://ftp.rfc-editor.org/in-notes/rfc3989.txt) .

Implementations

- Software
  - Astaro Security Linux (http://www.astaro.com/)
  - MCS Firewall - [1] (http://www.mcsstudios.com)
  - Check Point VPN-1 (formerly Firewall-1)
  - SC Gauntlet (discontinued, but still in use)
  - ipchains
  - Iptables
  - IPFilter (ipf)
  - ipfw
  - Microsoft Internet Security and Acceleration (ISA) Server (http://www.microsoft.com/isa/)
  - Netfilter/iptables
  - PF
  - WinGate Proxy / NAT Firewall (http://www.wingate.com)
  - PORTUS-APS
- Appliances
  - ActionTEC (a DSL Modem packaged by Qwest with new DSL customer orders)
  - Celestix MSA Series
  - Cisco PIX and Cisco ASA
  - CyberGuard
  - Global Technology Associates, Inc.
  - NetASQ
  - DataPower
  - Juniper NetScreen
  - Lightning MultiCom VPN Firewall - [2] (http://www.lightning.ch)
  - Lucent VPN Firewall - [3] (http://lucent.com/security)
  - Nortel Stand-alone and Switched Firewall - [4] (http://products.nortel.com/go/product_content.jsp?parId=0&segId=0&catId=-9460&prod_id=362

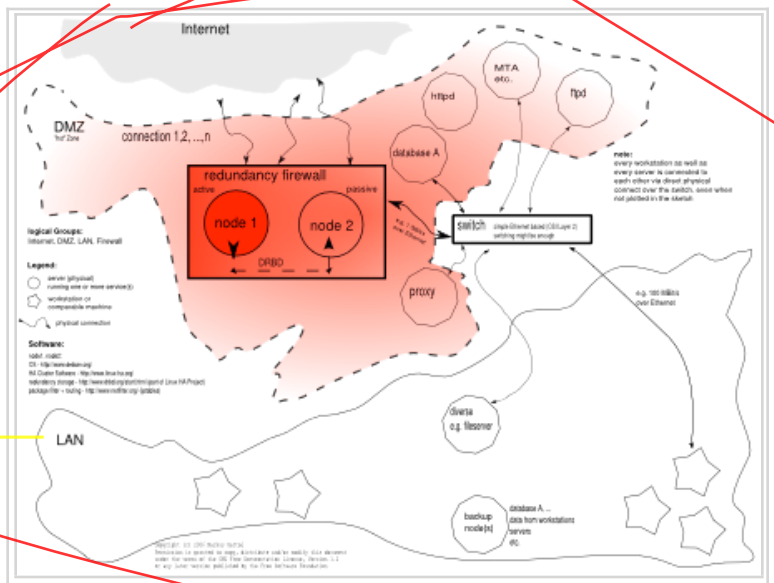
  - Phion NetFence
  - PORTUS-APS Appliance
  - Sarvega
  - Sidewinder and Sidewinder G2
  - SofaWare Technologies
  - XNet (Made in Pakistan) (Contact nadeem@xnet.com.pk)
  - SonicWall
  - Watchguard
- Free Software Distributions (that allows you to reuse your old computer as a firewall)
  - Endian Firewall (http://www.efw.it) (GPL)
  - IPCop (GPL)
  - m0n0wall (BSD-style license)
  - pfSense (BSD-style license) (m0n0wall fork)
  - Devil-Linux (GPL)
  - SmoothWall Express (GPL)
  - eBox Platform (GPL)
  - BrazilFW Firewall and Router (http://www.brazilfw.com.br/forum/portal.php) (GPL) - Formerly Coyote Linux - This runs from a floppy disk or hard disk, and is configured through a Windows or Linux program.

- Personal firewalls – see that article

Use case scenario

The simplest form could be like this:

- node 1 and node 2 running an OS with a Linux kernel (Debian GNU/Linux for example)
- To create a redundancy firewall we could choose to build a high-availability cluster. Therefore we need to connect those nodes (at least two are necessary) to each another in a way they could "see" each other. The software to do so could be Heartbeat (http://www.linux-ha.org/HeartbeatPrc which is part of Linux-HA Project
- The most critical task in such a scenario is to ensure that all nodes share the same data at all times, better known as data integrity. This could be done with DRBD which is roughly speaking nothing else than a network RAID 1.



A redundancy firewall reduces the possibility of an Internet connection Outage.

- Last but not least we need firewalling capabilities for the redundancy firewall. A packet filter like iptables helps here.

Online firewall check

These sites offer free online portscan services to check your firewall security. Please note that online port probes are not 100% bulletproof, as they always check the *public* IP address, which may be a proxy server. Online portscans are easy to use and offer basic insights, but to ensure network security, use tools like Nmap.

- ShieldsUP (Gibson Research Corporation) (https://www.grc.com/x/ne.dll?bh0bkyd2) Quick and easy to use
- Sygate Online Scan (http://scan.sygate.com/) Extended security check, concise (Stealth Scan, Trojan Scan)
- Planet Security Firewall-Check (http://www.planet-security.net/index.php?xid=%F7%04T%BDP%92nD) Quick, extended security check, checks current endangered ports, clearly laid out, TCP Scan

See also

- Middlebox
- Windows Firewall
- Firewall pinhole
- End-to-end connectivity
- Access control list
- Bastion host
- Demilitarized zone (DMZ)
- Great Firewall of China

External links

- Matt Curtin and Marcus J. Ranum Internet Firewalls: Frequently Asked Questions (http://www.faqs.org/faqs/firewalls-faq/)
- Evolution of the Firewall Industry (http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm) - Discusses different architectures and their differences, how packets are processed, and provides a timeline of the evolution.

Retrieved from "http://en.wikipedia.org/wiki/Firewall_%28networking%29"

Categories: Computer network security | Network-related software | Packets

---