The purpose of the **firewall** is to moderate traffic and/or log it. Most firewall are made for moderating ip traffic and are called **ip firewalls**.

The simplest ip firewall has two physical interfaces normally referred to as *inside* (LAN) and *outside* (WAN, the internet). It has two main access control lists (ACL) - e.g. named inside2outside and outside2inside.

Contents

- 1 Packet filter firewall
- 2 Statefull firewall
- 3 NAT - Network address Translation
    - 3.1 NAT incompatible protocols
- 4 Firewall difficult protocols
- 5 DD-WRT firewall - iptables
    - 5.1 Netfilter iptables architecture
- 6 See also
- 7 External links

Packet filter firewall

The simplest ip firewall - a packet filter firewall - can pass packet by packet or drop them based on:

- source ip address
- destination ip address
- If tcp or udp:
    - source tcp/udp port
    - destination tcp/udp port

Statefull firewall

The better ip firewall - a statefull firewall - can pass packet by packet - and if possible (e.g. tcp and udp) track the connection. A statefull firewall can additionally moderate trackable traffic by:

- number of connections per (src/dst) ip address
- number of connections per interface
- number of connections attempt - "SYN"-attacks, packet storms

NAT - Network address Translation

Due to IPv4 address shortage, the internet society began to use NAT, and therefore the firewall also need to be NAT aware.

NAT incompatible protocols

A real problem with NAT is when more than one inside clients (e.g. C1, C2) connect to the same outside server ip address (S) and the traffic is not tcp and udp. When a response outside packet later arrives at the NAT device (firewall), it can not deduce which client to send it to. Here are examples of protocols that has that problem:

- IPsec (over IP protocol 51)
- PPTP (over IP protocol 47)
- L2TP (over IP protocol 50)

Even if the traffic is unencrypted it can not be deduced where to NAT a response outside packet, if more than one inside client uses the same protocol to the same outside ip address. UDP and TCP are special because they have 65536 possible src and dst ports that can help connection tracking.

Firewall difficult protocols

Some protocols can in-line signal a port jump and/or create connections one or both ways "at will". A firewall that can moderate that kind of traffic, need to inspect the traffic stream. To do that a firewall must have transparent proxies and are then called an application firewall.

Some examples of protocols that can port jump and/or create additional connections are:

- FTP passive
- FTP active - if you enable proxy support for active FTP, you firewall can be "punctured" from the internet and is therefore almost useless.
- Media streams (Media Player, iTunes...):
    - ♦ RTSP
    - ♦ Realmedia
    - ♦ Conferencing
    - ♦ VoIP, IP telephony:
        - ◊ H323
        - ◊ SIP
- Some gaming protocols

DD-WRT firewall - iptables

DD-WRT has a packet filtering firewall, statefull firewall, NAT and proxy functionality.

The default internal device network has two networks (non-802.11n example!):

- vlan0(built-in hardware switch) software-bridged with eth1(wireless access point) - LAN private ip subnet 192.168.1.0/24 and ip configurations are leased to clients by a DHCP server.
- vlan1 - WAN with some ip configuration normally acquired via a DHCP client.

There is a default ip firewall with NAT between vlan0 and vlan1 (on non-802.11n) network devices.

See internal_device_network#Examples_of_changed_internal_network for other firewall examples.

Netfilter iptables architecture

- sns.ias.edu: Kernel space structure - simple packet journey through kernel
    - The left and right upper red arrows together, is the input and output of your network device logical network interfaces (bridges=switches, - and vlans). The five blue balls represent the default firewall chains hook points. The "local process" is your network device's service process(es) - e.g. remote management (WEB server, Telnet or SSH server), Samba server, PPPoE client, DHCP server(s) or client and so on.

See also

- DD-WRT Firewall Example
- iptables commands (written for DD-WRT)

External links

- Firewall Generic and short: Purpose and processes.
- sns.ias.edu, James Stephens: Iptables
    - IPTABLES - An Overview - short and good - overheads.
        - Kernel space structure - simple packet journey through kernel - Please note that the left and right upper red arrows together, is the input and output of your network device logical network interfaces.
    - Comprehensive and well documented NAT-less iptable and startup script:
        - Iptables example ruleset
        - A simple accompanying startup script
        - The updated ruleset may be downloaded
- wikipedia:Netfilter
    - netfilter.org: Documentation about the netfilter/iptables project, lists
    - people.netfilter.org: Netfilter Performance Testing
- interhack.net: Internet Firewalls: Frequently Asked Questions Good.
- Web archive backup (be patient): Kernel Packet Traveling Diagram Quote: "...On the LARTC mailing list, there was a long discussion about how a packet is handled by the kernel. Finally, there was a post by Leonardo Balliache that I copied onto this page. I hope this helps people to better understand how it all works....", **Good ASCII drawing of the ethernet/ip packet journey through the Linux Kernel**. Simplify the drawing for yourself, if you do not use some of the processes.
- Another good drawing of the ethernet/ip packet journey through the Linux Kernel with some actions written
- Iptables-tutorial - e.g. on-line:
    - Iptables Tutorial, Oskar Andreasson Good and very thorough.
- Ipsysctl-tutorial - e.g. on-line:
    - Ipsysctl tutorial, Oskar Andreasson, Good and very thorough.
- sans.org: SANS InfoSec Reading Room - Firewalls & Perimeter Protection notably:
    - Netfilter and IPTables: A Structural Examination Good.
- My Firewall Page - "A Firewall is a concept..." Quote: "...Generic Packet-Filter Ruleset...Keep in mind that these hints are for a single workstation-computer connected to the Internet..."
- Firewall Knowledgebase notably:
    - Setting up an iptables firewall

    - how to set firewall for linux
- DD-WRT Specific IPTables Info
- OpenWRT Advanced Firewall