Michael Ko - u5010095

Linux Firewall Tools Research

A list of Linux Firewall management software I investigated, with short descriptions and features.

1. SmoothWall

SmoothWall is an open source Linux firewall that runs on a machine as a Linux distribution. It acts as a gateway between a machine and the internet, basically acting as a layer on top of iptables. It has a highly configurable web-based interface, which is both powerful and easy to use. It is considered to be the most well-known Linux firewall manager.

Features of SmoothWall

- Supports LAN, DMZ, and wireless networks, plus external.
- Real time content filtering.
- HTTPS filtering.
- Supports proxies.
- Log viewing and firewall activity monitor.
- Traffic stats management on per IP, interface and visitor basis.
- Backup and restoration facility like.

2. IPCop Firewall

IPCop is an Open Source Linux firewall distribution similar to SmoothWall, given that it was started as a SmoothWall fork back in 2003 the similarities aren’t surprising. IPCop provides a well-designed web interface to manage the firewall. It also runs as a separate Linux distribution that sits on top of iptables.

Features of IPCop Firewall

- Its colour coded web interface allows you to monitor the performance Graphics for CPU, memory and disk as well as network throughput.
- It views and auto rotates logs.
- Multiple language support.
- Provides a very secure stable and easily implementable upgrade and add on patches.

3. Shorewall

Shorewall Firewall is a very popular open source firewall specialized for GNU/Linux. It is built upon the Netfilter system built into the Linux kernel that also supports IPV6. The Netfilter system also includes some API for interacting with iptables.

Feature of Shorewall

- Uses Netfilter’s connection tracking facilities for stateful packet filtering.
- Supports a wide range of routers/firewall/gateway applications.
- Centralized firewall Administration.
- A GUI interface with Webmin control Panel.
- Multiple ISP support, supports VPN.
- Very comprehensive API.
- Supports masquerading and port forwarding.

4. Uncomplicated Firewall (UFW)

UFW is the default firewall tool for Ubuntu servers; it is basically designed to lessen the complexity of the iptables firewall and makes it more user-friendly. There also exists a graphical user interface for UFW called GUFW. The purpose of UFW closely resembles the aim of our own project, that is building architecture to manage firewall rules which is both simple and easy to use.

Features of UFW

- Supports IPV6.
- Extended logging options with on/off facility.
- Status monitoring.
- Extensible framework, which can be integrated with applications.
- Easily add/remove/modify rules according to your needs.

5. pfSense

pfSense is another open source Linux firewall and a very reliable firewall for FreeBSD servers. It's based on the concept of stateful packet filtering. It offers a wide range of features that are normally only available on commercial firewalls.

Features of pfsense

- Highly configurable and upgraded from its web – based interface.
- Can be deployed as a perimeter firewall, router, DHCP & DNS server (so it is very flexible).
- Configured as wireless access point and a VPN endpoint.
- Traffic shaping and real time information about the server.
- Inbound and outbound load balancing.

6. Vuurmuur

Vuurmuur is another powerful Linux firewall manager built to manage iptables rules for your server or network. No prior iptables working knowledge is required to use Vuurmuur, so it is very user friendly to use and administrate. This firewall is also closely related to what our mini project entails, ie. The management of iptables firewall rules in an easy to use fashion.

Features of Vuurmuur

- Supports IPV6 as well as traffic shaping.
- Advanced monitoring features.
- Real time monitoring connection and bandwidth usage.
- Can be easily configured with NAT, and has anti-spoofing features.

7. IPFire

IPFire is an open source Linux based firewall for small office/home office (SOHO) environments. It's been designed to be modular and highly flexible. The IPfire community also took care of security and developed it as a stateful packet inspection (SPI) firewall.

Michael Ko - u5010095

Features of IPFire

- Can be deployed as a firewall, a proxy server or a VPN gateway.
- Content filtering.
- Inbuilt intrusion detection system.
- Support through Wiki, forums and online chat.
- Support of hypervisors like KVM, VmWare and Xen for virtual environments.

Michael Ko - u5010095

API Investigation

Most of the Linux firewall managers didn’t have much of an API to interact with or manage the firewall. There was one standout firewall manager that had a very comprehensive API list, this was Shorewall firewall. Shorewall can behave as gateway, firewall, router, server or as a standalone system. It is essentially a high-level tool for configuring Netfilter on firewall requirements, by using a set of configuration files. Netfilter then interacts with iptables to create a set of firewall rules associated with the Shorewall configuration files.

Shorewall supports JSON data serialization format. The format for both the request and the response should be specified by using the Content-Type header, the Accept header. Shorewall had the most comprehensive API list with an easy to understand scope and grammar, I think we would be smart to use something similar for our own project.

List of API

Verb	URI	Description
POST	/firewall/:group/shorewall	Create/update a new interfaces, zones, policy,shorewall.conf, tcdevices, tcclasses and capabilities file configurations in shorewall server
POST	/firewall/:group/tcrules	Create/update a new tcrules configurations on shorewall server
POST	/firewall/:group/masq	Create/update a new masq configurations on shorewall server
POST	/firewall/:group/rules	Create/update a new rules configurations on shorewall server
GET	/firewall/:group/shorewall	GET DB details of interfaces, zones, policy,shorewall.conf, tcdevices, tcclasses and capabilities file configurations in shorewall server
GET	/firewall/:group/tcrules	GET DB details of tcrules configurations on shorewall server
GET	/firewall/:group/masq	GET the DB details of masq configurations on shorewall server
GET	/firewall/:group/rules	GET the DB details of rules configurations on shorewall server
GET	/firewall/:group	GET the DB details of respective group configurations on shorewall server
DELETE	/firewall/:group/tcrules	DELETE the DB details and tcrules files configurations on shorewall server
DELETE	/firewall/:group/masq	DELETE the DB details and masq files configurations on shorewall server
DELETE	/firewall/:group/rules	DELETE the DB details and rules files configurations on shorewall server
DELETE	/firewall/:group/shorewall	DELETE the DB details and respective group

		configurations files on shorewall server
POST	/shorewall/server/:group/conf	Create/update a new shorewall.conf file configuarations for shorewall in shorewall server
POST	/shorewall/server/:group/zones/:id	Create/update a new shorewall zones configurations on shorewall server
POST	/shorewall/server/:group/interfaces/:id	Create/update a new shorewall interfaces configurations on shorewall server
POST	/shorewall/server/:group/policy/:id	Create/update a new shorewall policy configurations on shorewall server
POST	/shorewall/server/:group/rules/:id	Create/update a new shorewall rules configurations on shorewall server
POST	/shorewall/server/:group/routestopped/:id	Create/update a new shorewall routestopped configurations on shorewall server
GET	/shorewall/server/:group/conf	Describes an installed shorewall.conf file configurations in shorewall server
GET	/shorewall/server/:group/zones/:id	Describes the configurations of the shorewall zones file and DB by shorewall ID
GET	/shorewall/server/:group/interfaces/:id	Describes the configurations of the shorewall interfaces file and DB by shorewall ID
GET	/shorewall/server/:group/policy/:id	Describes the configurations of the shorewall policy file and DB by shorewall ID
GET	/shorewall/server/:group/rules/:id	Describes the configurations of the shorewall rules file and DB by shorewall ID
GET	/shorewall/server/:group/routestopped/:id	Describes the configurations of the shorewall routestopped file and DB by shorewall ID
GET	/shorewall/server/:group/zones	Describes the installed shorewall zones files configurations of cpn-client1
GET	/shorewall/server/:group/interfaces	Describes the installed shorewall interfaces files configuartions of cpn-client1
GET	/shorewall/server/:group/policy	Describes the installed shorewall policy files configurations of cpn-client1
GET	/shorewall/server/:group/rules	Describes the installed shorewall rules files configurations of cpn-client1
GET	/shorewall/server/:group/routestopped	Describes the installed shorewall routestopped file configuartions of cpn-client1
GET	/shorewall/server/:group	Describes the installed shorewall configurations of a shorewall-lite client
POST	/shorewall/client/:group/capabilities	To create capabilities file on shorewall-lite clients
GET	/shorewall/client/capabilities/:group	To get the capabilities file from shorewall-lite clients to orchestration
POST	/shorewall/capabilities/server/:group	Get the capabilities configs from orchestration to shorewall server

POST	/shorewall/server/:group/build	To compile(build) for firewall, firewall.conf files for clients in shorewall server
POST	/shorewall/server/:group/rebuild	To compile(rebuild) for firewall, firewall.conf files for clients in shorewall server
GET	/shorewall/server/firewall/:group/scripts	To get firewall and firewall.conf files from shorewall server to orchestration
POST	/shorewall/firewallfiles/client	To send the firewall and firewall.conf files from orchestration to shorewall-lite clients
POST	/shorewall/client/:group/start	To start the firewall rules on shorewall-lite clients
POST	/shorewall/client/:group/status	To get the status of firewall rules on shorewall-lite clients
POST	/shorewall/client/:group/stop	To stop the firewall rules on shorewall-lite clients
POST	/shorewall/client/:group/clear	To clear the firewall rules on shorewall-lite clients
POST	/shorewall/client/:group/restart	To restart the firewall rules on shorewall-lite clients
DELETE	/shorewall/server/:group/conf	Deletes the configurations of shorewall.conf file and entry in DB
DELETE	/shorewall/server/:group/zones/:id	Deletes the configurations of respective clients-groups shorewall ID
DELETE	/shorewall/server/:group/interfaces/:id	Deletes the configurations of respective clients-groups shorewall ID
DELETE	/shorewall/server/:group/policy/:id	Deletes the configurations of respective clients-groups shorewall ID
DELETE	/shorewall/server/:group/rules/:id	Deletes the configurations of respective clients-groups shorewall ID
DELETE	/shorewall/server/:group/routestopped/:id	Deletes the configurations of respective clients-groups shorewall ID

Michael Ko - u5010095

Important Features

Our project with Red Hat requires us to build and design architecture to manage firewall rules. We went and browsed internet discussion boards, open source requests and talked personally with Linux users and found some core features that people would like in such an architecture.

- Simple to both set up and administrate, ie. A firewall manager that works out of box.
- Ability to create default rules for known services.
- Clarity - firewall rules should be clear and uncomplicated (this is a problem with complicated iptables firewall rules).
- Comprehensive API list, with an easy to understand grammar and good scope.
- Easy to port to various different systems, not limited to just Linux.
- Firewall rules should only be applied on demand when the related service is running. They should then be removed when the service is no longer running.

References

Top 5 Best Linux Firewalls. 2014. Top 5 Best Linux Firewalls. [ONLINE] Available at: http://www.thegeekstuff.com/2010/02/top-5-best-linux-firewalls/.

7 of the best Linux firewalls | News | TechRadar. 2014. 7 of the best Linux firewalls | News | TechRadar. [ONLINE] Available at:http://www.techradar.com/au/news/software/applications/7-of-the-best-linux-firewalls-697177#articleContent.

10 Useful Open Source Security Firewalls for Linux Systems. 2014. 10 Useful Open Source Security Firewalls for Linux Systems. [ONLINE] Available at:http://www.tecmint.com/open-source-security-firewalls-for-linux-systems/.

Smoothwall - Internet Security and Content Filtering Solutions . 2014. Smoothwall - Internet Security and Content Filtering Solutions . [ONLINE] Available at: http://www.smoothwall.com/en-gb.

shorewall. 2014. shorewall. [ONLINE] Available at: https://www.npmjs.org/package/shorewall.

Netfilter - Wikipedia, the free encyclopedia. 2014. Netfilter - Wikipedia, the free encyclopedia. [ONLINE] Available at: http://en.wikipedia.org/wiki/Netfilter#iptables.