How-To Alpine Wall

From Alpine Linux

Contents

General

Purpose of this doc is to illustrate Alpine Wall (`AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)`) by examples.
We will explain `AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` from the viewpoint of a Shorewall user.

`AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` is available since Alpine v2.4.
Please see Alpine_Wall_User's_Guide for details about the syntax.

Some of the below features and examples assumes that you are running `AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` version 0.2.12 or later.
Make sure you are running latest version by running the following commands:

```
apk update
apk add -u awall
apk version awall
```

Structure

Your AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall) firewall configuration file(s) goes to /etc/awall/optional
Each such file is called *Policy*.

Note: AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall) versions prior 0.2.12 will only look for *Policy* files in /usr/share/awall/optional.
From version 0.2.12 and higher, AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall) will look for *Policy* files in both /etc/awall/optional and /usr/share/awall/optional

You may have multiple *Policy* files *(it is useful to have separate files for eg. HTTP,FTP and other roles)*.
The *Policy(s)* can be enabled or disabled by using the "awall [enable|disable]" command.

Note: AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)'s *Policy* files are not equivalent to Shorewalls /etc/shorewall/policy file.

An AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall) *Policy* can contain definitions of:

- variables *(like /etc/shorewall/params)*
- zones *(like /etc/shorewall/zones)*
- interfaces *(like /etc/shorewall/interfaces)*
- policies *(like /etc/shorewall/policy)*
- filters and NAT rules *(like /etc/shorewall/rules)*
- services *(like /usr/share/shorewall/macro.HTTP)*

Prerequisites

After installing AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall), you need to load the following iptables modules:

```
modprobe ip_tables
modprobe iptable_nat    #if NAT is used
```

This is needed only the first time, after AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall) installation.

Make the firewall autostart at boot and autoload the needed modules:

```
rc-update add iptables
```

A Basic Home Firewall

We will give a example on how you can convert a "Basic home firewall" from Shorewall to `AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)`.

Example firewall using Shorewall

Let's suppose you have the following Shorewall configuration:

/etc/shorewall/zones

```
inet  ipv4
loc   ipv4
```

/etc/shorewall/interfaces

```
inet  eth0
loc   eth1
```

/etc/shorewall/policy

```
fw   all  ACCEPT
loc  inet ACCEPT
all  all  DROP
```

/etc/shorewall/masq

```
eth0  0.0.0.0/0
```

Example firewall using AWall

Now we will configure `AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` to do the same thing as we just did with the above Shorewall example.

Create a new file called `/etc/awall/optional/test-policy.json` and add the following content to the file.

Tip: You could call it something else as long as you save it in `/etc/awall/optional/`

and name it `???.json`)

```
{
  "description": "Home firewall",

  "zone": {
    "inet": { "iface": "eth0" },
    "loc": { "iface": "eth1" }
  },

  "policy": [
    { "in": "_fw", "action": "accept" },
    { "in": "loc", "out": "inet", "action": "accept" }
  ],

  "snat": [
    { "out": "inet" }
  ]
}
```

The above configuration will:

- Create a description of your *Policy*
- Define *zones*
- Define *policy*
- Define *snat (to masqurade the outgoing traffic)*

Note: *snat* means "source NAT". It does not mean "static NAT".

Tip: `AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` has a built-in zone named "_fw" which is the "firewall itself". This corresponds to the Shorewall "fw" zone.

Activating/Applying a Policy

After saving the *Policy* you can run the following commands to activate your firewall settings:

```
awall list                  # Listing available 'Policy(s)' (This step is optional
awall enable test-policy    # Enables the 'Policy'
awall activate              # Genereates firewall configuration from the 'Policy'
```

If you have multiple policies, after enabling or disabling them, you need to always run *awall activate* in order to update the iptables rules.

Advanced Firewall settings

Assuming you have your `/etc/awall/optional/test-policy.json` with your "Basic

home firewall" settings, you could choose to modify that file to test the below examples.

> **Tip:** You could create new files in `/etc/awall/optional/` for testing some of the below examples

Logging

`AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` will *(since v0.2.7)* automatically log dropped packets.
You could add the following row to the "policy" section in your *Policy* file in order to see the dropped packets.

```
{ "in": "inet", "out": "loc", "action": "drop" }
```

> **Note:** If you are using Alpine 2.4 repository (`AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` v0.2.5 or below), you should use `"action": "logdrop"` in order to log dropped packets .

> **Note:** If you are adding the above content to an already existing file, then make sure you add "," signs where they are needed!

Port-Forwarding

Let's suppose you have a local web server (192.168.1.10) that you want to make accessible from the "inet".
With Shorewall you would have a rule like this in your `/etc/shorewall/rules`:

```
#ACTION  SOURCE  DEST              PROTO  DEST    SOURCE    ORIGINAL
#                                         PORT(S) PORT(S)   DEST
DNAT     inet    loc:192.168.1.10  tcp    80
```

Lets configure our `AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` *Policy* file likewise by adding the following content.

```
 "variable": {
   "APACHE": "192.168.1.10",
   "STATIC_IP": "1.2.3.4"
   },

 "filter": [
   { "in": "inet",
     "dest": "$STATIC_IP",
     "service": "http",
     "action": "accept",
```

```
    "dnat": "$APACHE"
    }
  ]
```

As you can see in the above example, we create a

- "variable" section where we specify some IP-addresses
- "filter" section where we do the actual port-forwarding (using the variables we just created and using some preexisting "services" definitions)

Note: If you are adding the above content to a already existing file, then make sure you add "," signs where they are needed!

Tip: `AWall (https://pkgs.alpinelinux.org/package/main/x86_64/AWall)` already has a "service" definition list for several services like HTTP, FTP, SNMP, etc. *(see `/usr/share/awall/mandatory/services.json`)*

If you need to forward to a different port (e.g. 8080) you can do:

```
"dnat": [
  {"in": "inet", "dest": "$STATIC_IP", "to-addr": "$APACHE", "service": "http", "to-port": 8080 }
]
```

Create your own service definitions

You can add your own service definitions into your *Policy* files:

```
"service": {
  "openvpn": { "proto": "udp", "port": 1194 }
  }
```

Note: You can not override a "service" definition that comes from `/usr/share/awall/mandatory/services.json`

Note: If you are adding the above content to a already existing file, then make sure you add "," signs where they are needed!

Inherit services or variables

You can import a *Policy* into other *Policy* files for inheriting services or variables definitions:

```
"import": "myfirewall"
```

Specify load order

By default policies are loaded on alphabetical order.
You can change the load order with the keywords "before" and "after":

```
"before": "myfirewall"
"after": "someotherpolicy"
```

Other

Help and debugging

If you end up in some kind of trouble, you might find some commands useful when debugging:

```
awall                 # (With no parameters) Shows some basic help about awall app
awall dump            # Dump definitions like zones and variables
iptables -L -n        # Show what's in iptables
```

Retrieved from "http://wiki.alpinelinux.org/w/index.php?title=How-To_Alpine_Wall&oldid=11267"

Categories: Networking | Security

- This page was last modified on 23 October 2015, at 08:02.
-