

Firewall Setup

Install Shorewall6

Configuring *Shorewall* for IPv6 is nearly identical to how I did it for IPv4. The biggest different is I can skip most things related to *masquerading* since that is less often necessary in the world of IPv6.

The only changes that need to be made is installing and configuring *shorewall6*. I am not going to go over everything again since it is nearly identical to [Firewall Setup](#) under IPv4 but pay close attention to the path is now `/etc/shorewall6`

```
# apt install shorewall6
```

```
# /etc/shorewall6/shorewall.conf
- LOG_LEVEL="info"
+ LOG_LEVEL="NFLOG(1,0,1)"
...
- LOGFILE=/var/log/messages
+ LOGFILE=/var/log/firewall.log
...
- IP_FORWARDING=Keep
+ IP_FORWARDING=Yes
```

```
# /etc/shorewall6/zones
+ #-----
+ # For information about entries in this file, type "man shorewall-zones"
+ #
+ # See http://shorewall.org/manpages/shorewall-zones.html for more information
+
#####
#####
+ #ZONE  TYPE  OPTIONS          IN          OUT
+ #
+ #          OPTIONS          OPTIONS
+ fw      firewall
```

```
+ wan    ipv4
+ lan    ipv4
+ dmz    ipv4
+ warp   ipv4
```

```
# /etc/shorewall6/interfaces
+ #-----
+ # For information about entries in this file, type "man shorewall6-interfaces"
+ #
+ # See http://shorewall.org/manpages/shorewall-interfaces.html for more information
+
#####
#####
+ ?FORMAT 2
+
#####
#####
+ #ZONE[]INTERFACE[]OPTIONS
+ wan[]WAN_IF[]tcpflags,dhcp,forward=1,accept_ra=2,sourceroute=0,physical=eth0
+ lan[]LAN_IF[]tcpflags,dhcp,forward=1,physical=eth1
+ dmz[]DMZ_IF[]tcpflags,dhcp,forward=1,physical=eth1.8
+ warp[]WARP_IF[]tcpflags,dhcp,forward=1,physical=eth1.9
```

```
# /etc/shorewall6/policy
+ #-----
+ # For information about entries in this file, type "man shorewall-policy"
+ #
+ # See http://shorewall.net/manpages/shorewall-policy.html for more information
+
#####
#####
+ #SOURCE[]DEST[]POLICY[]LOGLEVEL[]RATE  CONNLIMIT
+
+ $FW[]all[]ACCEPT
+ lan[]all[]ACCEPT
+ dmz[]$FW,wan[]ACCEPT
+ warp[]$FW[]ACCEPT
+
+ wan[]all[]DROP[]$LOG_LEVEL
+ # THE FOLLOWING POLICY MUST BE LAST
```

```
+ all[]all[]REJECT[]$LOG_LEVEL
```

```
# /etc/shorewall6/rules
+ #-----
+ # For information about entries in this file, type "man shorewall-rules"
+ #
+ # See http://shorewall.net/manpages/shorewall-rules.html for more information
+
#####
#####
#####
+ #ACTION[]SOURCE      DEST      PROTO DEST  SOURCE      ORIGINAL    RATE      USER/
MARK  CONNLIMIT  TIME      HEADERS  SWITCH  HELPER
+ #                                PORT  PORT(S)    DEST      LIMIT      GROUP
+ ?SECTION ALL
+ ?SECTION ESTABLISHED
+ ?SECTION RELATED
+ ?SECTION INVALID
+ ?SECTION UNTRACKED
+ ?SECTION NEW
+
+ #    Don't allow connection pickup from the net
+ Invalid(DROP)[]wan      all      tcp
+
+ DNS(ACCEPT)[]all!wan,warp  $FW
+ DNS(ACCEPT)[]$FW,dmz      lan:2001:db8:2fa3:4848::9a57:cec2
+
+ Web(ACCEPT)[]dmz          $FW
+ Web(ACCEPT)[]wan          dmz:2001:db8:2fa3:4848:66:1cb:59a7:bbe1
```

At this point I just have an empty `/etc/shorewall6/snat` configuration because IPv6 doesn't need masqueraded to access the Internet.

```
# /etc/shorewall/snat
+ #-----
+ # For information about entries in this file, type "man shorewall-snat"
+ #
+ # See http://shorewall.org/manpages/shorewall-snat.html for more information
+
#####
```

```
#####  
#####  
+ #ACTION          SOURCE          DEST          PROTO  PORT  IPSEC  MARK  USER  SWITCH  
ORIGDEST          PROBABILITY
```

Just like before it might be wise to run `shorewall6 check` just to make sure I didn't have any typos.

I already enabled *shorewall-init.service* to secure the system during boot so to hook in *shorewall6* I just needed to edit its configuration and then enable *shorewall6.service* to start at boot like I already did for *shorewall.service* and *shorewall-init.service*.

```
# /etc/default/shorewall-init  
- PRODUCTS="shorewall"  
+ PRODUCTS="shorewall shorewall6"
```

Then I told it to start at boot.

```
# systemctl enable shorewall6
```

Reboot

It isn't strictly necessary to reboot but I just prefer to see my system as it would be after it starts up.

```
# reboot
```

Revision #9

Created 31 March 2021 23:51:41 by dustin@swigg.net

Updated 8 April 2021 12:56:47 by dustin@swigg.net