

Keepalived LoadBalancing

LVS Config

```
## Pool ID
virtual_server <WAN "frontend" IP> 80 {
    delay_loop 6
    lb_algo sh      # source hash
    lb_kind NAT
    protocol TCP

    real_server <LAN "backend" IP Server 1> 80 {
        weight 1
        TCP_CHECK {
            connect_timeout 3
        }
    }
    real_server <LAN "backend" IP Server 2> 80 {
        weight 1
        TCP_CHECK {
            connect_timeout 3
        }
    }
}

virtual_server <WAN "frontend" IP> 443 {
    delay_loop 6
    lb_algo sh      # source hash
    lb_kind NAT
    protocol TCP

    real_server <LAN "backend" IP Server 1> 443 {
        weight 1
        TCP_CHECK {
            connect_timeout 3
        }
    }
    real_server <LAN "backend" IP Server 2> 443 {
```

```
        weight 1
        TCP_CHECK {
            connect_timeout 3
        }
    }
}
```

VRRP

```
vrrp_instance VI_LOCAL {
    state MASTER
    interface eth1
    virtual_router_id 51
    priority 101
    virtual_ipaddress {
        10.X.X.X
    }

    track_interface {
        eth0
        eth1
    }
}
```

```
vrrp_instance VI_PUB {
    state MASTER
    interface eth0
    virtual_router_id 52
    priority 101
    virtual_ipaddress {
        X.X.X.X
    }
    track_interface {
        eth0
        eth1
    }
}
```

```
vrrp_instance VI_PUB2 {
```

```

state MASTER
interface eth0
virtual_router_id 53
priority 101
virtual_ipaddress {
    X.X.X.X
}

track_interface {
    eth0
    eth1
}
}
}

```

sysctl

```

# Use ip that are not configured locally (HAProxy + KeepAlived requirements)
net.ipv4.ip_nonlocal_bind = 1

# Enable packet forwarding
net.ipv4.ip_forward=1

# Disables IP source routing
net.ipv4.conf.all.accept_source_route = 0

# Enable IP spoofing protection, turn on source route verification
net.ipv4.conf.all.rp_filter = 1

# Disable ICMP Redirect Acceptance
net.ipv4.conf.all.accept_redirects = 0

# Decrease the time default value for tcp_fin_timeout connection
net.ipv4.tcp_fin_timeout = 15

# Decrease the time default value for tcp_keepalive_time connection
net.ipv4.tcp_keepalive_time = 1800

# Enable TCP SYN Cookie Protection
net.ipv4.tcp_syncookies = 1

```

```
# Enable ignoring broadcasts request
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Enable bad error message Protection
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Log Spoofed Packets, Source Routed Packets, Redirect Packets
net.ipv4.conf.all.log_martians = 1

# Increases the size of the socket queue
net.ipv4.tcp_max_syn_backlog = 1024

# Increase the tcp-time-wait buckets pool size
net.ipv4.tcp_max_tw_buckets = 1440000

# Arp
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.all.arp_announce = 2
net.ipv4.conf.all.arp_ignore = 1
```

DR

```
vim /etc/modules
```

```
“ iptable_mangle
  xt_multiport
  xt_MARK
  ip_vs
  ip_vs_rr
  ip_vs_nq
  ip_vs_wlc
```

```
${IPTABLES} -t mangle -A PREROUTING -p tcp -d <VIP-WAN>/32 -j MARK --set-mark 0x1
```

Keepalived

```

virtual_server fwmark 1 {
    delay_loop 10
    lb_algo lc
    lb_kind DR
    protocol TCP
    persistence_timeout 28800

    real_server <WAN-WEB1> 0 {
        weight 1
        TCP_CHECK {
            connect_port 443
            connect_timeout 3
        }
    }
    real_server <WAN-WEB2> 0 {
        weight 2
        TCP_CHECK {
            connect_port 443
            connect_timeout 3
        }
    }
}

```

Revision #6

Created 6 March 2019 15:52:15

Updated 31 July 2019 04:41:13 by Dave