A primer to Zone-Based Firewall

Santiago Lorente - 2020-04-02 - 0 Comments - in Zone-based Firewall

This document is intended to serve as a quick introduction to Zone Based Firewall in VyOS. ZBF lets the network admin combine network interfaces into groups (Zones) and apply catch-all firewalling for inter-zone traffic.

Why

For most super basic use cases, ZBF is overkill. But when your network starts to get slightly more complex, and you start having several networks and vlans belonging to different zones, groups or tenants and you want do do rigid firewalling between the two, Your rulesets quickly start to get both repetitive, messy and hard to maintain. The solution? Enter Zone-based firewalling, or 'zone-policy'.

What

As opposed to regular per-interface firewall rulesets, zone-based policy, from a very basic standpoint, lets you combine several network interfaces into a group (Zone) and treat them as one. Also, it allows you to apply firewall rulesets in a zone-to-zone relation (Ie Trusted->DMZ or WAN->Tenant1) as opposed to just inbound and outbound from each interface.

A common example

A good example use case is a semi-enterprise environment with many local networks. The number of users have grown to the point where the admin needs to segregate his network into many smaller networks, without having to keep track of firewalling between all of them. Consider this list of example networks:

```
Internal networks
eth0.10    10.6.10.0/24        Engineering1
eth0.11    10.6.11.0/24        Engineering2
eth0.12    10.6.12.0/24        Engineering3
eth0.13    10.6.13.0/24        Sales1
eth0.14    10.6.14.0/24        Sales2

Services networks
eth0.100   10.6.100.0/24       Services1-1
eth0.101   10.6.101.0/24       Services1-2
```

```
eth0.102   10.6.101.0/24       Services1-3

Two different DMZs
eth0.1501    10.6.150.0/28      DMZ1-1
eth0.1502    10.6.150.16/28      DMZ1-1
eth0.1503    10.6.150.32/28      DMZ1-1
eth0.1504    10.6.150.48/28      DMZ1-1

eth0.1601    10.6.160.0/28      DMZ1-1
eth0.1602    10.6.160.16/28      DMZ1-1
eth0.1603    10.6.160.32/28      DMZ1-1
eth0.1604    10.6.160.48/28      DMZ1-1

A VPN link to, say, some other company
eth1.10     214.55.123.1/30    IPVPN-DaughterCompany

And your WAN service provider.
eth1.40     132.123.123.2/30   WAN
```

For example, you would want to make sure that the guys at engineering have access to the services running in the services networks, but the sales guys shouldn't. You want the guys coming from IPVPN to be able to access both DMZ1 and DMZ2, but only a few servies from DMZ1 should be available from WAN. And so on. And so forth. And ofcourse all groups/zones of networks (Ie sales guys, engineering, services etc) should have access to all networks within the same zone/group.

Doing this properly using the regular per-interface inbound/outbound approach amounts to an uncomfortable amount of ruleset clutter and repetition. Imagine if you could, for example, manage traffic to ALL the sales group from WAN, with a single ruleset? Well, you can. Enter ZBF.

How

As previously mentioned, in ZBF, we no longer deal with inbound and outbound rulesets per interface (or per zones). In fact we're going to make one ruleset per source/destination zone combo. That's going to be a lot of rulesets, but the good thing is each set will be very nice and tidy, and in reality, since inter-zone communication is always blocked by default, you're only going to create rulesets and zone 'from' definitions where you explicitly want to enable traffic between zones.

See Zone-policy_example for a practical example