Zone-Based Firewall

Every firewall has a rule set which says what kind of traffic is allowed or what should be blocked. The most simple method of doing that is simply attaching the rule to your interface. The interface kind be either virtual (VLANs) or physical.
Let's take a look at an example.

In the image below you can see that we have 2 networks. One is WAN (`eth0`), and the other is LAN (`eth1`).
If we want to drop all incoming traffic but accept outgoing we can simply write this.

```
set firewall name OUTSIDE-IN default-action 'drop'
set firewall name OUTSIDE-IN rule 10 action 'accept'
set firewall name OUTSIDE-IN rule 10 state established 'enable'
set firewall name OUTSIDE-IN rule 10 state related 'enable'

set interfaces ethernet eth0 firewall in name OUTSIDE-IN
```

This firewall configuration will simply drop all incoming traffic except traffic that is already established or traffic that was initiated via the client.

Now we are gonna add another network called, "DMZ" (`eth2`). This has Public IP-addresses and all traffic should be allowed. However with our current setup it will block it regardless. We would have to add a rule to the firewall accepting traffic of which the destination is DMZ. Simple, but what if we have yet another DMZ. Or we start having more network. Using firewalls and adding rules to one interfaces becomes a mess. And that is where the Zone Based Firewall (ZBF) comes to the rescue.

What is it?

In short, with ZBF you assign interfaces to a specific zone. On that zone you configure the firewall rules. In total you have three specific rules. Incoming, outgoing and local.