**Rule Set for Intrusion prevention system IPS**

For IPS rules we don’t need to create our own rules unless we know of certain traffic and want to monitor it. For good level of security IPS already provides us ruleset by many providers that have identified the attacks.

Figure 1: Suricata IPS Rule set

Table

Description automatically generated with medium confidence

This figure shows that I have downloaded and enabled the ruleset for SSL IP blacklist and Fingerprint Blacklist. The best technique would be to enable all the rulesets that are provided to enhance the security.

Once I have downloaded the ruleset, we can view the rules and change the action to “drop” or “alert” as shown in figure 2

Figure 2 Rules

Graphical user interface, application, table

Description automatically generated

**Rules for Firewall**

Now there are two firewalls in the network design, so we need to configure different set of rules for each firewall.

**Firewall 1**

It is the firewall that is placed after the IPS and needs to allow all the incoming traffic but block the outgoing traffic. It will have the following rules

Figure 3: Changing firewall default behavior

Graphical user interface, text, application, email

Description automatically generated

First change the default behavior of the firewall to block the outgoing traffic from the local area network as we don’t want the internal network traffic to go out.

Figure 4: WAN ruleset

Graphical user interface, application

Description automatically generated

Here are the rules that allow WAN traffic form any port and source to pass through the firewall but block the traffic form local area from going out.

**Firewall 2**

The second firewall is placed between internal network and DMZ it will allow the traffic form internal network to DMZ but block all the traffic from DMZ to enter the internal network.

Figure 5: WAN Ruleset

Graphical user interface, text, application

Description automatically generated

WAN rules will block all the incoming traffic.

Figure 6 LAN Ruleset

Graphical user interface, text, application

Description automatically generated

On the LAN we can allow the traffic on the DMZ that has the IP address 192.168.100.6 so requests will be allowed to the DMZ.