FW CNaaS Zones and Policies

Naming standards

Rules and zones should always have a describing name.

Example zone name: office

Example rule name: allow_icmp

SUNET specific zones always start with SUNET-

Zones

Zones are located under 'security zones' and consists of the interfaces that the zones are made for and what traffic thats allowed to talk directly to the firewall from that interface (host-inbound-traffic) and a description.

Example zone:

```
#> show configuration security zones security-zone office
description "office";
host-inbound-traffic {
   system-services {
      ping;
      dhcp;
   }
   protocols {
      bgp;
      bfd;
   }
}
interfaces {
   reth0.244;
}
```

Policies

Policies are the "rules" and are made out of a set of statements, going from one zone to another zone.
The firewall checks from the top of the list and if the first policy doesn't match it continues to the next, so position of the policies is important.

Example policy:

```
#> show configuration security policies from-zone office to-zone internet
policy allow_ping {
   match {
      source-address office-pfx;
      destination-address any;
      application icmp;
   }
   then {
      permit;
   }
}
policy deny_all {
   match {
      source-address any;
      destination-address any;
      application any;
   }
   then {
      reject;
      log {
         session-init;
      }
      count;
   }
}
```