JUNOS: Securing routing engine for out-of-band management

Purpose

Most JUNOS based equipment provides a dedicated management ethernet port to create a separate management network. This allows connection and management of the devices independent on the operation and access of the production network. This access does not prevent the remote access and management of the devices from the production network only provide the dedicated management network for access. This technique uses a firewall filter (stateless packet filters) to secure the device against access from the production network so that only management network access is permitted.

Solution

JUNOS provides firewall filters to restrict access to interfaces. These are stateless packet filters and not flow based firewall rules. Once a filter is created and applied there is a default deny all rule as the final action for the filter. So all permitted options must be specified or the final rule in the filter must be an allow all rule.

For the security of the device we need to create rules that allow only the management traffic from the management network and further rules that allow necessary routing information protocols from the production sources. To secure the routing engine firewall filters are applied to the loopback address.

In this example the loopback address is 192.168.0.254 and the management network is 192.168.0.0/24.

Firewall Filter Process

Using firewall filters is a two step process. The filter is created for general use in the firewall hierarchy. Then the filter is applied to the loopback interface at the interface hierarchy.

This filter will block ssh and telnet from anywhere except the management network. But allow all other traffic to the routing engine.

[edit firewall family inet]

dev@lab01# show

```
filter mgmt-filter {
    term allow-mgmt{
        from  {
            source-address {
                192.168.0.0/24;
            }
        }
        then {
            accept;
```

```
        }
    }
  term block-mgmt {
      from  {
          protocol  tcp{
              destination-port [ ssh telent ];
               }
        }
        then {
            reject;
         }
      }
      term accept-traffic {
          then accept;
       }
  }
```

Term "accept-traffic" options for routing engine traffic

The alternative to accepting all traffic is to specify in detail what protocols are actually used by this routing engine then only accepting this type of traffic. The default deny rule will then drop everything else. These are the items to add to the "accept-traffic" term stanza for specific protocols. Remember to only add those protocols needed from production. The first term already allows everything connecting from the management network.

For this application add a from stanza to accept-traffic term and include all the protocols needed from the production side networks.

```
  Term accept-traffic {
      from {
 add protocol list from table below
       }
      then {
         accept;
  }
```

Term to add in filter	Protocol allowed
protocol icmp; icmp-type [echo-request echo-reply time-exceeded unreachable];	Ping
protocol udp; ttl 1;	Traceroute
protocol udp; source-port 53;	DNS
protocol tcp; source-port bgp;	BGP
protocol ospf;	OSPF
protocol vrrp;	VRRP
protocol udp: source-port ntp;	NTP
protocol udp; source-port [snmp snmptrap];	SNMP

Apply Firewall Filter to Loopback address

The firewall filter is applied to the input of the loopback address.

```
interfaces {
   lo0 {
      unit 0 {
         family inet {
           filter {
              input mgmt-filter;
           }
           address 192.168.0.254/24;
           }
         }
      }
   }
```

JUNOS: Securing routing engine for out-of-band management

References

JUNOS Documentation

Configuring the Junos OS the First Time on a Router with a Single Routing Engine

http://www.juniper.net/techpubs/en_US/junos10.3/topics/task/configuration/routing-engine-single-initial-configuration.html

Connecting and Configuring an EX Series Switch (CLI Procedure)

http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/task/configuration/ex-series-initial-configuration-setting-up-cli.html

Configuring SSH Service for Remote Access to the Router or Switch

http://www.juniper.net/techpubs/en_US/junos10.2/topics/task/configuration/ssh-services-configuring.html

Loopback Interface Landing page

http://www.juniper.net/techpubs/en_US/junos10.3/information-products/pathway-pages/config-guide-network-interfaces/loopback-interface.html

JUNOS as a second language course

Chapter 9: Firewall Filters

https://learningportal.juniper.net/juniper/resources/courses/ed_serv/edu_jun_wbt_jsl_second/index.html

Knowledge Base Articles

Kb10880 - Configuring the management IP address on the EX-series switch

http://kb.juniper.net/InfoCenter/index?page=content&id=KB10880

Firewall Filter on loopback interface

http://kb.juniper.net/InfoCenter/index?page=content&id=KB12791