Cisco To Juniper

Thomas Mangin
Exa Networks
LINX 51

Scope

- This presentation is **not** about :
  - Juniper vs Cisco
  - A line per line conversion analysis
- It is about
  - Giving you an overview how hard/easy integrating Juniper in a Cisco network is ..
  - Providing you pointers should you want to look into it
  - Giving you a taste of the interesting feature of JunOS

Source of Information

- www.cymru.com
  - Secure Juniper BGP template
    - Complete tested template
    - Well documented
    - Very good to learn from an example
    - A little bit outdated
    - No IGP at all
    - Focused on security not features
  - Remotely triggered black hole example

Source of Information

- www.juniper.net
  - Cisco Configuration Converter
    - Good to get a base configuration and for IGP
    - Horrible (but correct) ACL and BGP route-map conversion
    - Access not open (you may have to ask your reseller to get your configuration converted)
  - Documentation
    - Cover clearly every section of the configuration
    - Have lots of configuration snipsets
    - Does not take you for a genius or a student of college
    - Is good enough to allow you to write configs from it

Source of Information

- juniper.cluepon.net
  - Wiki
  - password recovery procedure
  - Lots of unofficial information
  - Lots more ….
- nsp-juniper mailing-list
  - Lots of good configuration and discussion on the archive
  - Helpful juniper staff monitoring the list and answering “hard” questions.

The Routers

- Separation of the routing engine and forwarding plane
- BSD system on the background
  - Use unix commands (if you want)
    - ls, ps, top, tcpdump, compile your own
    - Every protocol has a daemon
  - Lots of HD space for logging
    - Usual risk associated with having an HD
    - Optional flash drive

Configuration

- Are looooooong …
  - Easily 2,000 lines for a EBGP routers
- But are very logical structure
  - Divided in “section”
  - From more generic to more specific
  - With the concept or “inheritance”
- Friendly
  - Everything can be commented
  - Everything can be “deactivated”
- Easy to manipulate
  - Merge/Replace/Overide from file/copy & paste/etc.
  - Export part of it/Save it all

Configuration

- Atomic changes
  - No time constrain to change the configuration
  - Automatic rollback if changes are not confirmed
- Automatic backup
  - possibility to rollback to any previous configuration version
  - Compare the current configuration with any stored backup
  - Export to ftp on change
- Changes are syntax checked
  - Can be a pain as it will not let you test a invalid configuration

Turn off the red light

- Juniper expect a management through the dedicated management internet interface.

```
chassis {
    alarm {
        management-ethernet {
            link-down ignore;
        }
    }
}
```

Policies

- The JunOS “route-map”
- Used to
  - Originate routes
  - Filter route to learn / announce
- Are
  - a succession of term (if then blocks)
    - Every keyword (term, from, then) if optional
  - terms can
    - Accept a route
    - Reject the route
    - Let the next policy decide
  - Policies be build from other policies

Policies - example

```
community drop-ebgp members [ 30740:65001 30740:65002 ];
community drop-ix members [ 30740:65003 30740:65004 ];

policy-statement export-bgp {
    term remove-ebgp {
        from {
            protocol bgp;
            community drop-ebgp;
        }
        then reject;
    }
    term remove-ix {
        from {
            protocol bgp;
            community drop-ix;
        }
        then reject;
    }
}
```

Policies with BGP

```
[edit protocol bgp]
group linx {
  type external;

  import [ no-ix no-bogons no-small-prefixes tag-linx damping local-preference-
     peer community-clear ];
  export [ originate export-peering export-linx community-clear next-hop-self ];

  neighbor 195.66.224.254 {
    apply-groups bgp-limit-50;
    description "LINX / Route Collector";
    authentication-key "$.....";
    peer-as 5459;
  }
}
```

Originate a route

- Filter can normally be chained allowing to reuse the power of other filters and thus making the configuration easier to maintain and more readable.
- However, originated routes need to be “accepted” in the filter where they are injected

Originate a route

```
routing-options {
    aggregate {
        route 82.219.0.0/16 community 30740:65400;
    }
}

policy-options {
    community originate members 30740:65400;
    policy-statement originate {
        term tag {
            from {
                protocol aggregate;
                community originate;
            }
            then {
                community delete originate;
                accept;
            }
        }
    }
}
```

(static route can as well be used instead of aggregate)

Groups

- JunOS allows to define configuration template
  - Can be used to define your interfaces common attribute (core, transit, peering, customers, …)
  - Abuse it to define BGP prefix-limit
  - Use “ | display inheritance “ allow to see implicitly what is explicit otherwise

Groups

```
groups {
  name {
    interfaces {
      <ge-*> {
        vlan-tagging;
        link-mode full-duplex;
          unit <*> {
            family inet {
              no-redirects;
} } } } } }
```

```
interfaces {
    apply-groups name;
    ge-0/3/0 {
        description “core vlan”
        unit 80 {
            apply-groups sub;
            vlan-id 18;
            family inet {
            /* Local comment */
            address 10.0.0.1/28;
} } } } }
```

Using BGP to setup firewall rules

- BGP and JunOS SCU can be use to build firewall rules from BGP tagged routes
- The same thing may be better done using Juniper flows implementation using the latest JunOS release.
- if interested see : http://www.atm.tut.fi/list-archive/juniper-nsp-20

Complain

- No easy way to see flow information
  - Like “show ip cache flow” with cisco
  - Need to capture the packet and pass them to the control plane which can then get overloaded and become unresponsive
  - Same issue with netflow export, a DDOS may not take the forwarding plane off but may overload the netflow daemon, causing IGP/BGP update drop.
  - Juniper sell some “hardware accelaration cards” to offload those tasks from the CPU
- Learning curve and all which goes with it.

Conclusion

- What problem did the introduction of Juniper caused ?
  - Full BGP table leak to one peer due to mis-configuration …
  - 5 minutes when the planned update to allow data flow collection obliged us to use out-of-band access to the router to rollback our changes
- All in one it went pretty well
- I would do it again …

Thank you

- for faking interest all the way through
  (or not)

- Questions ?
  (If times allow)