JUNOS Secure BGP Template

Version 1.92, 03/30/2005

Stephen Gill
E-mail: gillsr@cymru.com

Published: 04/25/2001

Contents

Credits

- Rob Thomas [robt@cymru.com] – author of Cisco Secure IOS BGP Template which this document was adapted from.
- B.K. Rogers
- John Kristoff
- Markus Åberg

Introduction

The following configuration was adapted from version 2.1 of the "Secure BGP Template" [5] presented by Rob Thomas. It was ported to JUNOS by Stephen Gill in order to serve as reference for those interested in simply configuring BGP on a Juniper router, or for those aiming at increasing the level of BGP stability and security in their network. A secure JUNOS configuration outline has been diverted to the "JUNOS Secure Template" [3].

The overall network topology assumed here is the same as that of the aforementioned template and should be fairly readable for those familiar with BGP. A brief diagram has been provided in Figure 1 for clarity. Though this template was written from the perspective of secure-router-01, it can be easily mirrored to reflect the secondary router.

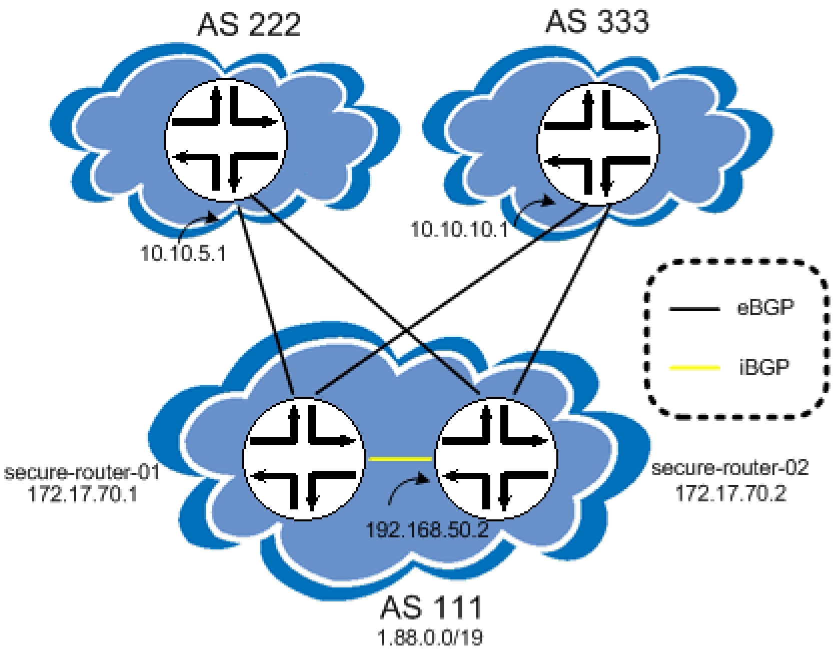

Figure 1 - Network Topology

This template was originally developed on a Juniper M10 running JUNOS 4.3R3. Since then, it has been field tested and approved by many engineers in the field, running several different versions of code on numerous hardware platforms. It is our intention to further enhance this tool and keep it up to date with current technologies. If you have any feedback or questions regarding this document, please forward them to gillsr@cymru.com.

General comments have been inserted using the 'annotate' feature to aid in deciphering some of what the configuration is doing. Formatting has also been rearranged for readability.

If you are familiar with BGP on a Cisco router, a few key items to note are the following:

- Juniper does not support the 'synchronization' feature since they feel that it is deprecated and should not be utilized. It is only necessary when redistributing BGP routes into your IGP and given the current size of the Internet routing table, it would probably not be a wise idea to pursue this route.
- Soft reconfiguration is always on. Routes learned from neighbors and routes advertised to peers are stored in conjunction with the local BGP table. IE. adj-rib-In and adj-rib-out are resident in memory along with the loc-rib by default. One can easily view these tables by issuing the following commands:

show route receive-protocol bgp <neighbor> – displays Adj-RIB-In
show route advertising-protocol bgp <neighbor> – displays Adj-RIB-Out
show route protocol bgp – displays Loc-RIB

Please consult the JUNOS documentation for further information on configuring BGP. The documentation set can be found at: http://www.juniper.net.

Template

A web tool that can automatically convert this template or any other JUNOS "function" style configuration into more CLI friendly "*set*" commands is available at: http://www.cymru.com/gillsr/tools.html. You may be able to save some typing by pasting your template into the conversion tool. A more direct approach to loading this configuration that does not require conversion can also be accomplished by using the "*load merge term*" command at the appropriate tree level and pasting the configuration directly into the router.

```
/* ... begin template ... */
version 4.3R3;
/* JUNOS 4.3R3 Secure BGP template */
routing-options {
    options {
        /* Turn off DNS resolution */
        no-resolve;
    }
    static {
        /* This is our aggregate static route */
        route 1.88.0.0/19 discard;
        /* More specific routes used with discard route above.  Remove these
           if using an IGP to discover internal routes. */
        route 1.88.50.0/24 next-hop 192.168.50.5;
        route 1.88.55.0/24 next-hop 192.168.50.8;
        route 1.88.75.128/25 next-hop 192.168.50.10;
        /* Route to loopback of our iBGP peer */
        route 172.17.70.2/32 next-hop 192.168.50.2;
        /* Black-hole routes for traffic destined to these networks */
        /* Use: http://www.cymru.com/gillsr/documents/junos-discard-
            routes.txt
        /*
    }
    /* Our AS Number */
    autonomous-system 111;
    /* Export the policy that turns on flow based load balancing */
    forwarding-table {
       export load-balancing;
    }
    /* Keep certain announcements from entering the routing table,
       but permit specific discard routes to remain there.  Use
       'show route martians' to view them. */
    martians {
        /* Use: http://www.cymru.com/gillsr/documents/junos-martians.txt */
    }
}
/* Routing protocol configuration */
protocols {
    bgp {
        /* Log additional BGP information to aid in troubleshooting.  To
           view, use 'show log log-bgp' */
        traceoptions {
            /* Rotate through 5 files at 1mb each */
            file log-bgp size 1m files 5;
            /* Trace BGP state transitions */
            flag state;
            /* Trace BGP normal events */
            flag normal;
        }
        /* Log BGP neighbor changes */
        log-updown;
        /* Enable bgp route flap damping */
        damping;
        /* Keep private AS numbers 64512-65535 from leaking out */
        remove-private;
        family inet {
            any {
                /* MUST take into account current routing table size and keep
                   a CLOSE watch on this.  Otherwise do NOT use!  Prefit
                   limits can be applied at the group level instead if
                   desired. */
                prefix-limit {
                    /* Tear down connection when routes reach maximum */
                    maximum 130000;
                    /* Start issuing warning messages at teardown percent */
                    teardown 90;
                }
            }
        }
        /* iBGP peer-group with AS 111.  Peer-groups save typing and CPU
           cycles when multiple neighbors exist with same policy */
        group iBGP_111 {
            type internal;
            description "iBGP with AS 111";
            /* Set my address to that of lo0 */
            local-address 172.17.70.1;
            authentication-key bgpwith111;
            /* Set next-hop-self for eBGP routes sent to our iBGP peer */
            export next-hop-self;
            /* The following is assumed if not entered */
            peer-as 111;
            /* Loopback address of our internal peer */
            neighbor 172.17.70.2;
        }
        /* eBGP peer-group with AS 222 */
        group eBGP_222 {
            type external;
            description "eBGP with AS 222";
            authentication-key bgpwith222;
            /* Inbound filtering: Remove bogons, small prefixes, private ASN
                advertisements, and set damping parameters. */
            import [ nobogons nosmallprefixes noprivateasns damping ];
            /* Only announce our netblock */
            export announce;
            peer-as 222;
            /* Allow installation of equal cost BGP paths into inet.0
               (routing table), one of which is then selected at random */
            multipath;
            neighbor 10.10.10.1;
        }
        /* eBGP peer-group with AS 333 */
        group eBGP_333 {
            type external;
            description "eBGP with AS 333";
            authentication-key bgpwith333;
            import [ nobogons nosmallprefixes noprivateasns damping ];
            export announce;
            peer-as 333;
            multipath;
            neighbor 10.10.5.1;
        }
    }
}
/* Route filtering configuration */
policy-options {
    /* List of root-servers.net as of 09/11/01.
       Refer to RIPE-229 [6] on keeping this list current. */
    prefix-list root-servers.net {
        128.8.0.0/16;
        128.9.0.0/16;
        128.63.0.0/16;
        192.5.4.0/23;
        192.33.4.0/24;
        192.36.148.0/24;
        192.112.36.0/24;
        192.203.230.0/24;
        193.0.14.0/24;
        198.32.64.0/24;
        198.41.0.0/24;
        202.12.27.0/24;
    }
    /* Match what we configured as our static aggregate netblock */
    policy-statement announce {
        term 1 {
            from {
                protocol static;
                route-filter 1.88.0.0/19 exact;
            }
            then accept;
        }
        term 2 {
            then reject;
        }
    }
    /* Martians list will reject bogon routes not listed here. Don't want
       multicast address range listed in the martian list.  */
```

```
policy-statement nobogons {
    from route-filter 224.0.0.0/4 orlonger reject;
}
/* Reject advertisements that contain private AS numbers. */
policy-statement noprivateasns {
    from as-path private;
    then reject;
}
/* AS-PATH referenced in the noprivateasns policy. */
as-path private 64512-65535;
/* Drop prefixes larger than /27.  Other BGP policies may vary */
policy-statement nosmallprefixes {
    from route-filter 0.0.0.0/0 prefix-length-range /27-/32 reject;
}
/* Set next-hop to self.  Used for eBGP routes sent to iBGP peers */
policy-statement next-hop-self {
    then {
        next-hop self;
    }
}
/* Configure load balancing.  IP1 ASIC performs packet load balancing on
   up to 8 equal cost paths.  IP2 ASIC performs flow based load balancing
   on up to 16 equal cost paths.  Use only if you have an IP2 ASIC. */
policy-statement load-balancing {
    then {
        load-balance per-packet;
  }
}
/* Configure our damping policy according to RIPE-229 and an updated set
   of DNS netblocks. */
policy-statement damping {
    /* Do NOT dampen DNS root-servers */
    term 1 {
        from {
            prefix-list root-servers.net;
        }
        then {
            damping damp-none;
            /* Ignore rest of terms and jump to next policy called */
            next policy;
        }
    }
    /* Dampen according to prefix length.  JunOS penalises on withdraw
       and on readvertise. So one flap attracts a total penalty of 2000.
       An attribute change attracts a penalty of 500. */
    term 2 {
        from {
            /* Lower penalty for prefixes of size /21 and smaller */
            route-filter 0.0.0.0/0 upto /21 damping damp-short;
            /* Medium penalty for prefixes of size /22 to /23 */
            route-filter 0.0.0.0/0 upto /23 damping damp-medium;
            /* Higher penalty for prefixes of size /24 and larger */
            route-filter 0.0.0.0/0 orlonger damping damp-long;
        }
        then {
            next policy;
        }
        }
    }
    /* Min: 30 min, Max: 60 min, dampen at 3 flaps */
    damping damp-long {
        half-life 30;
        reuse 1640;
        suppress 6000;
        max-suppress 60;
    }
    /* Min: 15 min, Max: 45 min, dampen at 3 flaps */
    damping damp-medium {
        half-life 15;
        reuse 1500;
        suppress 6000;
        max-suppress 45;
    }
    /* Min: 10 min, Max: 30 min, dampen at 3 flaps */
    damping damp-short {
        half-life 10;
        reuse 3000;
        suppress 6000;
        max-suppress 30;
    }
    /* Do not dampen.  Referenced for DNS root-servers */
    damping damp-none {
        disable;
    }
}
/* Firewall filtering rules need to be applied to an interface.  In this case
   it should be merged with existing firewall policy and applied to lo0. */
firewall {
    filter router-protect {
        /* Drop and log all unexpected BGP connection attempts */
        term 1 {
            from {
                address {
                    0.0.0.0/0;
                    10.10.5.1/32 except;
                    10.10.10.1/32 except;
                    172.17.70.1/32 except;
                    172.17.70.2/32 except;
                }
                protocol tcp;
                port bgp;
            }
            then {
                  count manage-discard-bgp;
                  discard;
            }
        }
        term 2 {
            then {
                /* Allow all other traffic */
                count manage-accept-other;
                accept;
            }
        }
    }
}

/* ... end template ... */
```

References

[1] Juniper, "Fortifying the Core", September 2000.
http://www.juniper.net/techcenter/app_note/350002.html

[2] Juniper, "Minimizing the Effects of DoS Attacks", November 2000.
http://www.juniper.net/techcenter/app_note/350001.html

[3] Gill, Stephen, "JUNOS Secure Template", October 2001.
http://www.cymru.com/gillsr/documents/junos-template.pdf

[4] Thomas, Rob, "Secure IOS Template", June 2001.
http://www.cymru.com/Documents/secure-ios-template.html

[5] Thomas, Rob, "Secure BGP Template", June 2001.
http://www.cymru.com/Documents/secure-bgp-template.html

[6] RIPE, "RIPE Routing-WG Recommendations for Coordinated Route-flap Damping Parameters", October 2001.
http://www.ripe.net/ripe/docs/ripe-229.html

[7] Thomas, Rob, "Bogon List", July 2002.
http://www.cymru.com/Documents/bogon-list.html