JUNOS Secure 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 Template which this document was adapted from.
- B.K. Rogers
- John Kristoff

Introduction

The following configuration was adapted from version 2.3 of the “Secure IOS Template” [5] presented by Rob Thomas. It was ported to JUNOS by Stephen Gill in order to serve as reference and starting point for those interested in increasing the level of security on their Juniper routers, and in return, their network. Quite a few aspects of security are covered, but each user will need to modify the template to fit his or her individual needs. A secure BGP configuration outline has been diverted to the “JUNOS Secure BGP Template” [3].

The overall network configuration assumed here is the same as that in the aforementioned template. A brief diagram has been provided in Figure 1 for clarity.

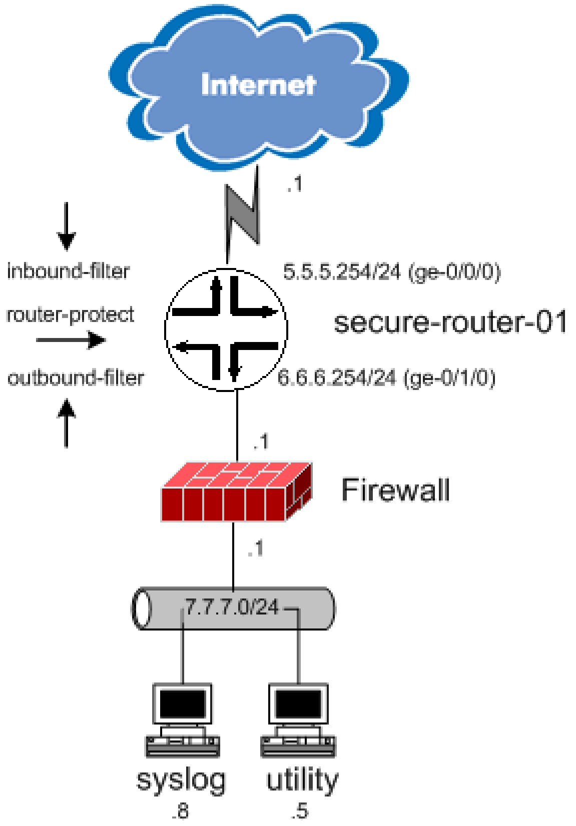

Figure 1 - Network Topology

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.

Please consult the JUNOS documentation for further information on configuring your Juniper router. The documentation set along with other helpful publications 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;
system {
    host-name secure-router-01;
    /* Enable a backup router during boot for ntp.  It will be used before
       rpd has started or if it fails. */
    backup-router 6.6.6.1 destination 7.7.7.0/24;
    time-zone America/Chicago;
    /* Do not send ICMP redirects */
    no-redirects;
    /* Use local password authentication if AAA fails */
    authentication-order [ radius password ];
    location country-code US;
    /* Configure authentication passwords */
    diag-port-authentication {
        encrypted-password "<PASSWORD>"; # SECRET-DATA
    }
    root-authentication {
        encrypted-password "<PASSWORD>"; # SECRET-DATA
    }
    /* Enable RADIUS authentication. Read ‘JUNOS RADIUS Authentication’ [4]
       for further information on configuring and troubleshooting RADIUS */
    radius-server {
        7.7.7.5 {
            /* Shared secret between client and server */
            secret "<PASSWORD>"; # SECRET-DATA
            /* Wait 5 seconds until timeout */
            timeout 5;
        }
    }
    login {
        /* Same as MOTD banner in Cisco.  Extend a stern introduction. */
        message "********************************************************\n
                 * [WARNING] secure-router-01                           *\n
                 * This system is owned by [COMPANY]. If you are not    *\n
                 * authorized to access this system, exit immediately.  *\n
                 * Unauthorized access to this system is forbidden by   *\n
                 * company policies, national, and international laws.  *\n
                 * Unauthorized users are subject to criminal and civil *\n
                 * penalties as well as company initiated disciplinary  *\n
                 * proceedings.                                         *\n
                 *                                                      *\n
                 * By entry into this system you acknowledge that you   *\n
                 * are authorized access and the level of privilege you *\n
                 * subsequently execute on this system. You further     *\n
                 * acknowledge that by entry into this system you       *\n
                 * expect no privacy from monitoring.                   *\n
                 ********************************************************\n";
        /* Configure an account classes with specific privileges.  We cannot
           modify the predefined classes, so we must create our own. */
        class tier1 {
            /* Session will time out after 15 minutes of inactivity */
            idle-timeout 15;
            /* Provides basic read-only privileges */
            permissions [ configure interface network routing snmp system
                          trace view firewall ];
        }
        class tier2 {
            idle-timeout 15;
            /* Provides a controlled subset of read-write privileges */
            permissions [ admin clear configure interface interface-
                          control network reset routing routing-control
                          snmp snmp-control system system-control trace
                          trace-control view maintenance firewall
                          firewall-control secret rollback ];
        }
        class tier3 {
            idle-timeout 15;
            /* Provides unlimited access */
            permissions all;
        }
        /* This is our local superuser account with a local password. */
        user admin {
            full-name Administrator;
            uid 2000;
            class tier3;
            authentication {
                encrypted-password "<PASSWORD>"; # SECRET-DATA
            }
        }
        /* RADIUS template tier1 user.  Read-only */
        user tier1 {
            uid 2001;
            class tier1;
        }
        /* RADIUS template tier2 user.  Read-write limited */
        user tier2 {
            uid 2002;
            class tier2;
        }
        /* RADIUS template tier3 user.  Read-write */
        user tier3 {
            uid 2003;
            class tier3;
        }
    }
    /* List of IPs and their hostnames */
    static-host-mapping {
        /* Put localhost entry for NTP to work */
        localhost inet 127.0.0.1;
        firewall-ext inet 6.6.6.1;
        firewall-int inet 7.7.7.1;
        upstream inet 5.5.5.1;
        utility inet 7.7.7.5;
        syslog inet 7.7.7.8;

    }
    /* Enable router services */
    services {
        /* Enable 5 ssh sessions.  Max 10 connection attempts per minute. */
        ssh connection-limit 5 rate-limit 10;
        /* JUNOS 5.0 and above: disallow remote root logins */
        root-login deny;
        /* JUNOS 5.0 and above: use SSH version 2 only */
        protocol-version v2;
    }
    syslog {
        /* Archive old files up to 10mb total */
        archive size 1m files 10;
        user * {
            any emergency;
        }
        /* Punt log data over to our syslog server */
        host 7.7.7.8 {
            any info;
        }
        file messages {
            any notice;
            authorization info;
        }
    }
    /* Synchronize our clock with a trusted authenticated NTP server */
    ntp {
        authentication-key 6767 type md5 value "<PASSWORD>"; # SECRET-DATA
        /* NTP will not sync if times are too distant.  Set time at bootup */
        boot-server 7.7.7.5;
        server 7.7.7.5;

    }
}
chassis {
    /* Disable source routing */
    no-source-route;
}
interfaces {
    /* Log additional interface information to aid in troubleshooting.  To
       view, use 'show log log-interfaces' */
        traceoptions {
            /* Rotate through 5 files at 1mb each */
            file log-interfaces size 1m files 5;
            /* Trace changes that produce configuration events */
            flag change-events;
    }
    ge-0/0/0 {
        description "Upstream Interface - facing Internet";
        /* Enable snmp-traps for this interface */
        traps;
        link-mode full-duplex;
        unit 0 {
            family inet {
                /* Do not send ICMP redirects */
                no-redirects;
                /* Filter inbound packets from the Internet */
                filter {
                    input inbound-filter;
                }
                address 5.5.5.254/24;
            }
        }
    }
    ge-0/1/0 {
        description "Protected Interface - facing DMZ"
        traps;
        link-mode full-duplex;
        unit 0 {
            family inet {
                no-redirects;
                /* Filter outbound packets from the internal network */
                filter {
                    input outbound-filter;
                }
                address 6.6.6.254/24;
            }
        }
    }
    /* Configure management interface.  Can NOT route over this. */
    fxp0 {
        description "Management Interface – OOB management"
        unit 0 {
            family inet {
                no-redirects;
                address 10.10.11.11/24;
            }
        }
    }
    /* Configure loopback interface.  Used for routing protocols and other
       purposes. */
    lo0 {
        description "Loopback Interface – internal"
        unit 0 {
            family inet {
                no-redirects;
                /* Restrict connections coming to this router */
                filter {
                    input router-protect;
                }
                address 10.10.10.10/32;
            }
        }
    }
}
forwarding-options {
    /* Enable packet sampling for CflowD */
    sampling {
        input {
            family inet {
                /* Sample 1 out of 100 packets + next 4 in sequence.
                   Total = 4/100 packets.  You may want to just sample
                   the SYN/FIN packets instead. */
                rate 100;
                run-length 4;
                /* This is a built-in max throttle, listed here for
                   completeness */
                max-packets-per-second 7000;
            }
        }
        /* Send our output to the designated CflowD collector using v 8 */
        output {
            cflowd 7.7.7.5 {
                port 2055;
                version 8;
                no-local-dump;
                autonomous-system-type origin;
                aggregation {
                    autonomous-system;
                }
            }
        }
    }
}
snmp {
    description secure-router-01;
    location "Site, Row, Rack, Shelf";
    contact "(555) 555-5555";
    /* Restrict SNMP requests to a particular interface */
    interface ge-0/1/0.0;
    /* Configure our SNMP community.  Replace COMMUNITY with your string */
    community COMMUNITY {
        authorization read-only;
        /* Determine who is allowed access via SNMP */
        clients {
            default restrict;
            /* Restrict access to ALL but the following */
            7.7.7.5/32;
        }
    }
    /* Send traps using v2 for all categories to designated trap server */
    trap-group all {
        version v2;
        categories authentication chassis link routing startup;
        targets {
            7.7.7.5;
        }
    }
}
routing-options {
    options {
        /* Turn off DNS resolution */
        no-resolve;
        syslog {
            level debug;
        }
    }
    /* Configure static routes */
    static {
        /* Default out to the Internet */
        route 0.0.0.0/0 next-hop 5.5.5.1;
        /* Route to network on the other side of the Firewall */
        route 7.7.7.0/24 next-hop 6.6.6.1;
        /* Use: http://www.cymru.com/gillsr/documents/junos-discard-
            routes.txt
        /*

    }
}
policy-options {
    prefix-list iana-reserved {
        /* Use: http://www.cymru.com/gillsr/documents/junos-reserved-prefix
            list.txt
        /*
    }
    prefix-list rfc1918 {
        /* RFC 1918 addresses */
        10.0.0.0/8;
        192.168.0.0/16;
        172.16.0.0/12;
    }
    /* Addresses to be used in router-protect-hardcore filter */
    prefix-list ssh-connect {
        6.6.6.1/32;
        7.7.7.5/32;
        7.7.7.8/32;
    }
    /* No BGP is used in this topology, but we allow it for future use */
    prefix-list bgp-connect {
        5.5.5.1/32;
    }
    prefix-list utility-connect {
        7.7.7.5/32;
    }
}
firewall {
    filter inbound-filter {
        /* Rate-limit for 5m/s used for multicast */
        policer udp-5m {
            if-exceeding {
                bandwidth-limit 5m;
                burst-size-limit 375k;
            }
            then discard;
        }
        /* Rate-limit for 500k/s used for ICMP */
        policer icmp-500k {
            if-exceeding {
                bandwidth-limit 500k;
                burst-size-limit 62k;
            }
            then discard;
        }
        /* Rate-limit for 2m/s used for UDP */
        policer udp-2m {
            if-exceeding {
                bandwidth-limit 2m;
                burst-size-limit 250k;
            }
            then discard;
        }
        /* The first three terms have been separated for accounting only */
        term 1 {
            from {
                source-address {
                    /* Spoof of inside networks */
                    6.6.6.0/24;
                    7.7.7.0/24;
                }
            }
            then {
                /* Count spoofed traffic.  Type 'show firewall' to view */
                count spoof-inbound-internal;
                discard;
            }
        }
        /* The following prefix-list can be divided for finer granularity */
        term 2 {
            from {
                prefix-list {
                    iana-reserved;
                }
            }
            then {
                count spoof-inbound-iana;
                discard;
            }
        }
        term 3 {
            from {
                prefix-list {
                    rfc1918;
                }
            }
            then {
                count spoof-inbound-rfc1918;
                discard;
            }
        }
        /* Discard all ICMP fragments */
        term 4 {
            from {
                is-fragment;
                protocol icmp;
            }
            then {
                count icmp-fragments;
                discard;
            }
        }
        /* Rate-limit ICMP traffic to 500k/s */
        term 5 {
            from {
                protocol icmp;
            }
            then {
                count policer-icmp-500k;
                policer icmp-500k;
            }
        }
        /* Rate-limit Multicast traffic to 5m/s */
        term 6 {
            from {
                destination-address {
                    224.0.0.0/4;
                }
                protocol udp;
            }
            then {
                count policer-multicast-5m;
                policer udp-5m;
                accept;
            }
        }
        /* Rate-limit other UDP traffic to 2m/s */
        term 7 {
            from {
                protocol udp;
            }
            then {
                count policer-udp-2m;
                policer udp-2m;
            }
        }
        /* Allow access to Intranet (Firewall filters specific ports) */
        term 8 {
            from {
                destination-address {
                    7.7.7.0/24;
                }
            }
            then accept;
        }
        /* Our explicit (read: logged) drop all rule */
        term 9 {
            then {
                discard;
            }
        }
    }
    /* Be a good netizen by preventing spoofing from within our network.
       You may wish to add further 'terms' if more access is required. */
    filter outbound-filter {
        term 1 {
            from {
                source-address {
```

```
                7.7.7.0/24;
                6.6.6.1/32;
            }
        }
        then accept;
    }
    term 2 {
        then {
            count spoof-outbound;
            discard;
        }
    }
}
/* You may apply this filter outbound on lo0 to count and compare
   SYN, RST, FIN, and other TCP traffic.  This can be used to detect a
   packet flood if you suspect you are under attack.  As an example, a
   high 'packets-syn' to 'packets-tcp' ratio could be a good indicator.
   TCP-intercept is not supported. */
filter tcp-flood-detect {
    term 1 {
        from {
            protocol tcp;
            tcp-flags syn;
        }
        then {
            count packets-syn;
            log;
            accept;
        }
    }
    term 2 {
        from {
            protocol tcp;
            tcp-flags rst;
        }
        then {
            count packets-rst;
            log;
            accept;
        }
    }
    term 3 {
        from {
            protocol tcp;
            tcp-flags fin;
        }
        then {
            count packets-fin;
            log;
            accept;
        }
    }
    term 4 {
        from {
            protocol tcp;
        }
        then {
            count packets-tcp;
            accept;
        }
    }
}
/* Two filters are supplied for protecting the RE: router-protect and
   router-protect-hardcore.  The first is easier to manage, but does
   not rate limit traffic to the RE and allows exception traffic by
   default.  The second is more secure but much more difficult to manage.
   Customize and apply only one of the router-protect filters inbound on
   lo0. You may wish to add entries for FTP, VRRP, TACACS, DNS, etc... */
filter router-protect {
   /* Allow SSH from firewall, syslog, and utility server */
    term 1 {
        from {
            source-address {
                0.0.0.0/0;
                6.6.6.1/32 except;
                7.7.7.5/32 except;
                7.7.7.8/32 except;
            }
            protocol tcp;
            destination-port ssh;
        }
        then {
            count manage-discard-tcp;
            discard;
        }
    }
    /* Allow access from designated SNMP, NTP, and RADIUS */
    term 2 {
        from {
            source-address {
                0.0.0.0/0;
                7.7.7.5/32 except;
            }
            protocol udp;
            port [ snmp ntp radius ];
        }
        then {
            count manage-discard-udp;
            discard;
        }
    }
    /* We only like the ICMP traffic listed below.  All other types are
       logged, counted, and discarded */
    term 3 {
        from {
            protocol icmp;
            icmp-type-except [ echo-request echo-reply unreachable
                               time-exceeded source-quench ];
        }
        then {
            count manage-discard-icmp;
            discard;
        }
    }
    /* We are not running BGP here but reserve this for future use */
    term 4 {
        from {
            address {
                0.0.0.0/0;
                5.5.5.1/32 except;
            }
            protocol tcp;
            port bgp;
        }
        then {
              count manage-discard-bgp;
              discard;
        }
    }
    term 5 {
        then {
            /* Allow all other traffic */
            count manage-accept-other;
            accept;
        }
    }
}
/* Now for a more secure, but tedious RE filter.  Remember to apply one
   of the router-protect filters inbound on lo0.  May need to account
   for traffic such as VRRP, FTP, OSPF, ISIS, or DNS here as well */
filter router-protect-hardcore {
    policer ssh-1m {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 100k;
        }
        then discard;
    }
    policer icmp-1m {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 100k;
        }
        then discard;
    }
    policer utility-3m {
        if-exceeding {
            bandwidth-limit 3m;
            burst-size-limit 300k;
        }
        then discard;
    }
    policer tcp-control-1m {
        if-exceeding {
              bandwidth-limit 1m;
              burst-size-limit 100k;
        }
        then discard;
    }
    /* Rate limit TCP control traffic from trusted sources */
    term 1 {
```

```
    from {
        source-prefix-list {
           ssh-connect;
           bgp-connect;
        }
        protocol tcp;
        tcp-flags "(syn & !ack) | fin | rst";
    }
    then {
        policer tcp-control-1m;
        accept;
    }
}
/* We are not running BGP here but reserve this for future use.
   Do NOT police this! */
term 2 {
    from {
        source-prefix-list {
            bgp-connect;
        }
        protocol tcp;
        port bgp;
    }
    then {
          accept;
    }
}
/* SSH is allowed from trusted servers only */
term 3 {
    from {
        source-prefix-list {
            ssh-connect;
        }
        protocol tcp;
        destination-port ssh;
    }
    then {
        policer ssh-1m;
        accept;
    }
}
/* SNMP, NTP, and RADIUS from trusted servers only */
term 4 {
    from {
        source-prefix-list {
            utility-connect;
        }
        protocol udp;
        port [ snmp ntp radius ];
    }
    then {
        policer utility-3m;
        accept;
    }
}
/* Block unwanted ICMP traffic, and rate-limit the rest */
term 5 {
```

```
            from {
                protocol icmp;
                icmp-type [ echo-request echo-reply unreachable time-exceeded
                             source-quench ];
            }
            then {
                policer icmp-1m;
                accept;
            }
        }
        /* Deny and log all other traffic */
        term 6 {
            then {
                count manage-discard-other;
                discard;
            }
        }
    }
}

/* ... 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 BGP Template", October 2001.
http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf

[4] Gill, Stephen, “JUNOS RADIUS Authentication”, November 2001.
http://www.cymru.com/gillsr/documents/junos-radius-authentication.pdf

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

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

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