# INTRODUCTION

## Rationale

An out-of-box firewall implementation is not fully secure and needs to be hardened. This document details the various aspects of Juniper firewall security and standards implemented for securing Juniper firewalls.

## Purpose

This document is to define a baseline security standard for the Juniper Firewall implementations by firewall administrators.

## Scope

These security standards cover the Juniper Firewall Screen OS implementation.

However, for some setups, this minimum requirement and some features of these standards may not be practical for implementation. For exceptions, the system administrators must document the reasons for not complying fully with these standards and request an exemption from the Security department.

## Audience

Firewall administrators bear the primary responsibility of implementing these standards. During their reviews and inspections, auditors must use this document to verify standards compliance.

Business managers can read the rationale behind each of the points in the standards to gain an understanding of the importance of applying it to their environments.

## Implementation

The Juniper Firewall administrators must use these standards to build the installation and operational procedures.

### Juniper Firewall Security Overview

This section gives a very brief overview of various aspects of Juniper Firewall security. The hardening details for each aspect are present in the subsequent sections of the document.

The Juniper Firewall operating security environment consists of various aspects:

- Device & ScreenOS initial setup
- Device Configuration
- Device Management
- User management
- Services
- System access
- System logging and monitoring
- Policy logging and monitoring

## DEVICE AND SCREENOS SETUP

The security of a Juniper firewall Screen OS starts with a secure setup. The factors that influence this include using the correct Screen OS version.

### Properly Identify Device for Physical Tampering

The outside packaging cannot show damage, or evidence that unauthorized persons have opened it. If the cardboard shows damage that would allow the device to be unpacked or exchanged, this may be evidence of tampering.

Each packed box arrives with custom tape to indicate that Juniper or an authorized manufacturer packaged the device. The tape is unique; with the word, “Juniper” printed repeatedly throughout the tape. If the tape is not present, this may be evidence of tampering.

The internal packaging cannot show damage or evidence of tampering. The plastic bag should not have a large hole and the label that seals the plastic bag should not be detached or missing. Any damage to the bag or the seal may be evidence of tampering.

### Verify correct version of hardware and software

To verify that the product received is the correct version of hardware and software, run the following command from the CLI:

```
get system
```

The output of this command includes two key items, hardware version and software version. The hardware and software versions must match the common criteria security target to be in full compliance with the common criteria evaluated configuration.

The firewalls come with pre-installed Screen OS software. However, the Screen OS software versions installed on the devices might vary depending on the manufacturing time of the security appliances.

## Upgrading a Juniper Firewall

The correct Screen OS software image needs to be loaded on to the security appliance.

Before the Screen OS software image can be loaded, configure the manage interface though which the images can be downloaded from the FTP server to the security appliances. The following commands will configure the zone and IP address for the manage interface.

**set interface** *interface-name* **zone** *trust*

**set interface** *interface-name* **ip** *ip-address*

*Note: Interface-name should the name of the actual interface connected to the PC serving as FTP firewall; through this interface, the security appliances can communicate with the FTP firewall. For the 5-series devices, interface* ***trust –*** *bound to the security zone* ***trust*** *by default – can be used. For devices Juniper NetScreen-204 and 208, you can use interface* ***ethernet1****. For Juniper NetScreen-500, interface ethernet1/1 in the security zone* ***trust*** *can be in place of interface-name. On high-level security, appliances including Juniper NetScreen-ISG2000 and ISG1000 interface can use ethernet1/1. Juniper NetScreen-5200 and NetScreen 5400 can use Interface ethernet2/1.*

The *ip-address* should be a valid IP address, which can be in the same or different subnet with the TFTP firewall.

Once configured, use the following commands to download the Screen OS image from the FTP firewall to the security appliance:

**save software from tftp** *tftp-firewall-ip Screen OS-image* **to flash**

where, *tftp-firewall-ip* is IP address for PC serving as the TFTP firewall where the Screen OS software images reside and, *Screen OS-image* is relative path to the Screen OS software image file and the name of the file itself.

For example, if the Screen OS image for the device Juniper NetScreen-5GT is “ns5gt.5.4.0r4.0” and resides on FTP firewall (with IP address 10.155.95.253), under the directory /tftpboot/screen OS-image/5.4/, the command should be as the following:

```
save software from tftp 10.155.95.253 /tftpboot/screenOS-image/5.4/ns5gt.5.4.0r4.0 to flash
```

The downloading process will take a few minutes. After the downloading process is completed, the security appliance will return to the CLI prompt and requires a reboot. Issue the command **reset** and provide answers for the questions below to completely load the image to the security appliance and restore the default manufacture configurations.

```
reset

Configuration modified, save? [y]/n n

System reset, are you sure? y/[n] y
```

The security appliance will return to the login prompt. At this time, the security appliance has been completely loaded with the proper Screen OS software version.

### Screen OS Upgrades

Update the firewalls' Screen OS with the vendor recommended updates as part of quarterly.

## DEVICE CONFIGURATION

### Restore default settings

Restore the firewall to the default manufacturing operation mode and configurations before putting the appliance in a different operation modes including Transparent Authenticated mode (a.k.a. Transparent VPN mode) or NAT/Route Authenticated mode (a.k.a. NAT/Route VPN mode) or before performing any configurations for any specific testing.

Use the commands **unset all** and **reset** along with the following answers to restored the default operation mode and configurations for the appliance.

```
unset all

Erase all system config, are you sure y/ [n]? Y

reset

Configuration modified, save? [y]/n n
```

**System reset, are you sure? y/[n] y**

**Set accurate date and time**

Enable the following command to ensure that the date and time stamps used on audit messages are accurate:

```
set clock mm/dd/yyyy hh:mm
```

## Setting the Operation Mode

To determine which operation mode the juniper firewall is, use the following command.

```
get system
```

“System in NAT/Route mode” indicates it is operating in NAT/Route mode

“System in transparent mode” indicates it is operating in transparent mode.

All security appliances are, by default, configured in NAT/Route mode without VPN.

<u>To ensure that a security appliance is in a mode compliant with the Common Criteria EAL4 evaluated configuration, follow one of the following three sets of steps depending on the desired configuration:</u>

- **Unauthenticated NAT/Route Mode**
- **Authenticated NAT/Route Mode**
  - **Route-Based VPN**
  - **Policy-Based VPN**
- **Authenticated Transparent Mode**

## Authenticated NAT/Route Mode

Configure the firewall in authenticated NAT/Route Mode using either a Route-based VPN or Policy-based VPN. You can configure both Route-based VPN and Policy-based VPN in authenticated NAT/Route mode.

Only Manual Key is supported in the Evaluated Configuration, i.e. AutoKey cannot be used. Take care in selecting Manual Key values such that they follow the same rules as administrative passwords. Distribute the manual keys using a secure method to ensure that they are not publicly accessible.

### Route-Based VPN

Configure the respective security appliance with a Route-based VPN in authenticated NAT/Route mode.

### Policy-Based VPN

Configure the respective security appliance with a Policy-based VPN in authenticated NAT/Route mode.

### Firewall Naming Convention

Branch Firewalls: (Naming convention not set)

Data Center Firewalls: (Naming convention not set)

### Configuring Screen Options

Security appliances must prevent all types of Denial of Service (DoS) and attack signatures on every security zone to prevent these types of attacks from occurring on the network.

To view the default screening options for a particular security zone, issue the following command.

**get zone** *zone-name* **screen**

By default, the screening options enabled for the **Untrust/V1-Untrust** security zone (and the interfaces in **Untrust/V1-Untrust** zone) in Screen OS 5.0:

**Tear-drop Attack Protection on**

**SYN Flood Protection (200) on**

**Alarm Threshold: *alarm-threshold***

**Queue Size: *Q-size***

**Timeout Value: 20**

**Source Threshold: *src-threshold***

**Destination Threshold: *dst-threshold***

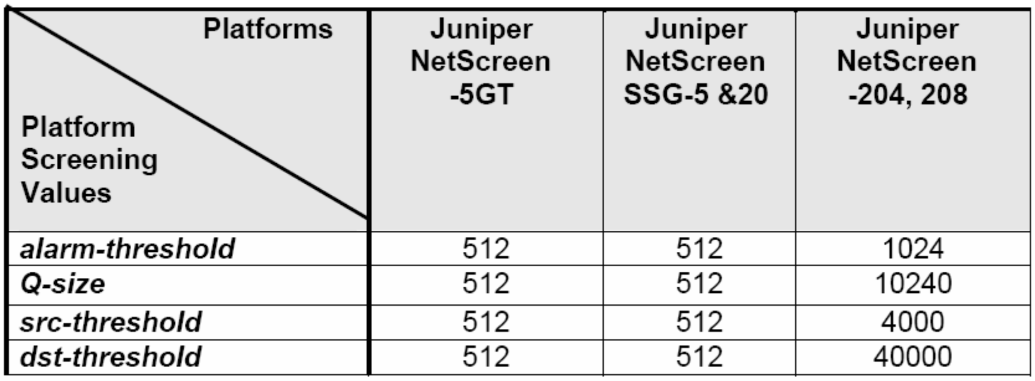
**Drop unknown MAC (transparent mode only): off**

**Ping-of-Death Protection on**

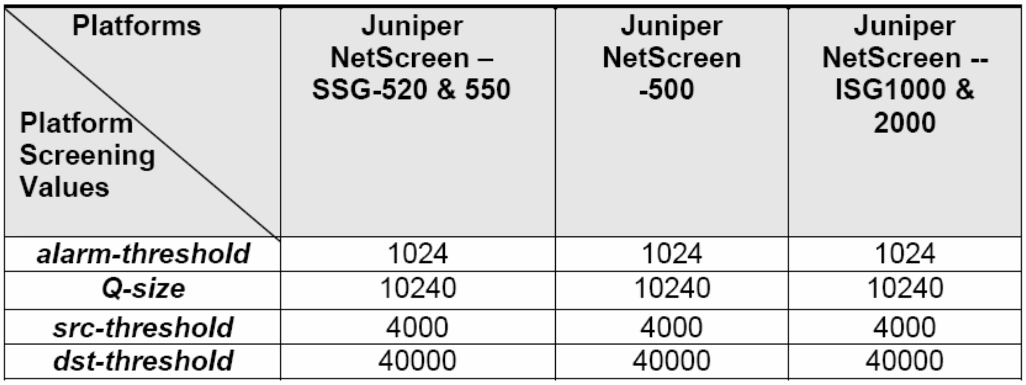
**Source Route IP Option Filter on**

**Land Attack Protection on**

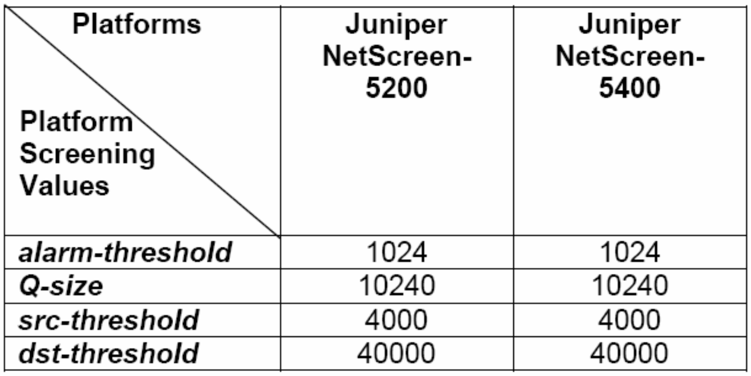
***Alarm-threshold, Q-size, src-threshold,*** and ***dst-threshold*** are platform dependent as specified in the table below.



| Platforms<br>Platform Screening Values | Juniper NetScreen -5GT | Juniper NetScreen SSG-5 &20 | Juniper NetScreen -204, 208 |
|---|---|---|---|
| *alarm-threshold* | 512 | 512 | 1024 |
| *Q-size* | 512 | 512 | 10240 |
| *src-threshold* | 512 | 512 | 4000 |
| *dst-threshold* | 512 | 512 | 40000 |



| Platforms<br>Platform Screening Values | Juniper NetScreen – SSG-520 & 550 | Juniper NetScreen -500 | Juniper NetScreen -- ISG1000 & 2000 |
|---|---|---|---|
| *alarm-threshold* | 1024 | 1024 | 1024 |
| *Q-size* | 10240 | 10240 | 10240 |
| *src-threshold* | 4000 | 4000 | 4000 |
| *dst-threshold* | 40000 | 40000 | 40000 |



| Platforms<br>Platform Screening Values | Juniper NetScreen-5200 | Juniper NetScreen-5400 |
|---|---|---|
| *alarm-threshold* | 1024 | 1024 |
| *Q-size* | 10240 | 10240 |
| *src-threshold* | 4000 | 4000 |
| *dst-threshold* | 40000 | 40000 |

For the **Trust/V1-Trust** and **DMZ/V1-DMZ** zones (and the interfaces in **Trust** and **DMZ** zone), no screen options are enabled by default.

**Screen function only generate alarm without dropping packet: OFF**

To disable all the default screening option for zone **Untrust/V1-Untrust,** the following commands are used:

```
unset zone untrust screen tear-drop
unset zone untrust screen syn-flood
unset zone untrust screen ping-death
unset zone untrust screen ip-filter-src
unset zone untrust screen land
```

The following displays when the security zone has no screening options enabled:

```
“Screen function only generate alarm without dropping packet: OFF”
```

The following CLI command enables all screens on a per-zone basis (and is applied to all interfaces within that zone):

```
set zone zone-name screen block-frag
set zone zone-name screen component-block
set zone zone-name screen fin-no-ack
set zone zone-name screen icmp-flood
set zone zone-name screen icmp-fragment
set zone zone-name screen icmp-large
set zone zone-name screen ip-bad-option
set zone zone-name screen ip-filter-src
set zone zone-name screen ip-loose-src-route
set zone zone-name screen ip-record-route
set zone zone-name screen ip-security-opt
set zone zone-name screen ip-spoofing
set zone zone-name screen ip-stream-opt
set zone zone-name screen ip-strict-src-route
set zone zone-name screen ip-sweep
set zone zone-name screen ip-timestamp-opt
set zone zone-name screen land
set zone zone-name screen limit-session
set zone zone-name screen mal-url code-red
set zone zone-name screen ping-death
set zone zone-name screen port-scan
set zone zone-name screen syn-ack-ack-proxy
set zone zone-name screen syn-fin
set zone zone-name screen syn-flood
set zone zone-name screen syn-frag
set zone zone-name screen tcp-no-flag
set zone zone-name screen tear-drop
set zone zone-name screen udp-flood
set zone zone-name screen unknown-protocol
set zone zone-name screen winnuke
```

The above commands must run for both the internal and external zones (i.e. Trust and Untrust) to protect the internal and external networks. When security appliance runs in NAT/Route mode, run the above commands for security zones **Trust** and **Untrust.**

When the security appliance runs in “Transparent” mode, (including Transparent Authenticated mode), run the above commands for security zones **V1-Trust** and **V1-Untrust.**

You must run the same commands (as above) for each additional security zone.

When the security appliance operates in NAT/Route mode, (including NAT/Route Unauthenticated and Nat/Route Authenticated mode) enable dropping packets that have no source IP address, or that have a non-routable source IP address by using the following command.

```
set zone zone-name screen ip-spoofing drop-no-rpf-route
```

*“zone-name”* is the name of the security zone such as **Trust** or **Untrust**.

For instance, when the security in NAT/Route mode, to turn on dropping packets capability for the security zone **trust** and **untrust**, issue the following commands.

```
set zone trust screen ip-spoofing drop-no-rpf-route
set zone untrust screen ip-spoofing drop-no-rpf-route
```

Ensure to execute the same command (as above) for any Layer-3 security zones that are used. When changing the HTTP blocking option the changes will only apply to the sessions newly created after this blocking option is set.

### Configuring IP Spoofing Protection

Configure IP spoofing protection by the screen option “ip-spoofing” as indicated above in the section, “Configuring Screen Options”. This includes **Intrazone** configurations where VPN traffic is on the same zone as the decrypted traffic. However depending on the configuration implemented (especially **Interzone**) the following additional steps are required to be adequately protected against IP spoofing attacks.

The following guidance for Authenticated NAT/Route mode and Authenticated Transparent mode should supplement the guidance provided in the previous section “Setting a Policy to Permit Traffic”.

"IP-Spoofing" Screen is bypassed - a set of addresses and policies need to be defined to allow only traffic permitted, excluding spoofed IP addresses.

When operating in Authenticated NAT/Route mode or Authenticated Transparent mode, the “IP-spoofing” screen option is “bypassed”. Therefore, define a set of addresses and policies to allow traffic, excluding spoofed IP addresses.

## DEVICE MANAGEMENT

This sections provides details on securing the firewall device’s management aspects

### Securing Administrator Traffic On Device

Four steps are required to secure the device administrator traffic:

a) Define permitted IP address for client administrator Manager-IP address

b) Define interface-specific options

   i) Define Manage IP address for interfaces

   ii) Turn off unnecessary management services

c) Change port numbers for administrator services

### Disable Internal Commands

The firewall administrator must disable internal commands. The usage of internal commands applies only for troubleshooting and debugging purposes.

To disable internal commands, you must run the following command:

```
set common-criteria no-internal-commands
```

To use internal commands (i.e. '**debug flow basic**' and '**get dbuf stream**', 'debug ids sat') for troubleshooting and debugging purposes, use the following command:

```
unset common-criteria no-internal-commands
```

*Note: Use the internal commands 'debug ids sat' is for ISG-1000, ISG-2000, NS-5200 and NS-5400*

### Disable Telnet for Device Management

The use of telnet is discouraged on the Juniper firewalls. Use SSH, 2.0 for managing the Juniper firewall:

To do this:

**Disable telnet on the management interface**

**Enable ssh**

### Control Unauthorized Hardware Resets

To disable recovery via login, use the following command:

```
unset admin device-reset
```

To disable recovery via pinhole, use the following command:

```
unset admin hw-reset
```

When disabled, a firewall administrator needs to enable the respective reset in order to perform any activity, which requires rebooting the firewall.

### Restricting Remote Access

Management access must be limited to the locally connected console port as opposed to the factory default settings.

To limit management access to the console port, the interface that is by default in the **V1-Trust** or **Trust** security zone needs to have management access turned off.

All other interfaces have management access turned off by default.

To disable management to the interface, issue the following CLI command:

**unset interface** *interface-name* **manage**

## USER MANAGEMENT

Security appliance administrators must choose login-names and passwords that not only have the length of at least eight characters and employ as many types of characters as possible. Mixing lower case and upper case is required to ensure proper protection. In addition, easily guessable usernames and passwords are not secure.

Security appliances ship with a default username and password of “netscreen”. Change the default as soon as possible to prevent unauthorized access.

The recommended time between password changes is no longer than 30 days to mitigate the effects of a compromised administrator identity.

### Setting/Changing Password Length Restrictions

To ensure that passwords of eight characters or more are always used, you must first set the following command:

**set admin password restrict length** *password-length*

where, *password-length* is a decimal value equal to or greater than 8 and less than or equal to 31. It should also follow password policy.

### Setting/Changing Administrator Name and Password

The following CLI commands, in order, are required to set a new administrator name and password:

**set admin name** *name-string*

**set admin password** *password-string*

where, *name-string* and *password-string* should be replaced with actual login name and password of administrator.

## POLICY MANAGEMENT

### Remove Permissive Default Policy

The firewall might have a default policy that allows traffic to traverse the device from the interface in the **Trust** zone to the interface in the **Untrust** zone. Delete this default policy to avoid inadvertently allowing information to traverse the device. Use the CLI command:

**unset policy id 1**

### Log Denied Traffic

By default, security appliance will drop any traffic that does not match any “permit” policy. Therefore, add a policy to the end of the policy list to log denied traffic, which matches no policy:

**set policy id** *pol-id* **from** *scr-zone* **to** *dst-zone* **any any any deny log**

**count**

…where, *pol-id* is policy ID, *scr-zone* and *dst-zone* are, respectively, source zone from which the traffic comes and destination zone to which the traffic arrives.

For every security zone that has a network interface assigned to it, add the above policies to the end of the policy tables to ensure that dropped traffic logging.

**set policy id** *pol-id* **from trust to untrust any any any deny log count**

**set policy id** *pol-id* **from untrust to trust any any any deny log count**

**set policy id** *pol-id* **from trust to dmz any any any deny log count**

**set policy id** *pol-id* **from dmz to trust any any any deny log count**

**…**

### Setting a Policy To Permit Traffic

Two important steps to take when creating a security policy:

- Enable counting and logging to maintain audit log information for traffic passing through the device.
- Must be specific to ensure traffic permitted is intentional and not part of a generic policy.

Use specific source IP address (*src-addr)*, destination IP address (*dst-addr)*, source zone (*src-zone)*, destination zone (*dst-zone)*, protocol, and service (*servicename)* if feasible. One example where it may not make sense to be specific is for traffic destined for an external network for general web access.

After creating and configuring the source and destination addresses, configure the policy with counting and logging using the following command:

**set policy id** *id-num* **from** *src-zone* **to** *dst-zone src-addr dst-addr servicename action* **log count**

…where, *"id-num"*: is the decimal number presenting the policy ID number & *"action*" can be **permit** to allow specific service to pass from source address across the security appliance to the destination address; or **deny** to block service from passing though the security appliance

### Ordering Policies

The order of policies is important, as policies match in order beginning with the first one in the policy list and moving through the list. The first matching policy applies to network traffic to determine the action taken. By default, a newly created policy appears at the bottom of a policy list.

There is an option that allows you to position a policy at the top of the list instead. In the CLI, add the key word **top** to the **set policy** command:

For example,

**set policy id** *6* **top from trust to untrust** *trust-HostA untr-NetworkB* **http permit log**

The newly created policy can also be positioned at any location in the policy list by using the keyword option **before** to the **set policy** CLI command.

For example:

```
set policy id 4  before 98 from untrust to trust untr-NetworkB trust-HostA ftp permit log
```

If global policies are used then replace the above policy, which executes prior to any Global policy. A Global deny policy can be used which must be added at the end of the Global policy list

```
set policy global id pol-id any any any deny log count
```

## System Logging and Monitoring

### Configuring Syslog

You should configure a Syslog firewall as a backup for security audit information and for long-term audit log storage. This will help prevent a loss in security audit information.

The specific commands required to set up a Syslog firewall are:

```
set syslog config ip-address facilities local0 local0

set syslog config ip-address port 514

set syslog config ip-address log traffic

set syslog enable

set log module system level level-name destination syslog
```

where *ip-address* is the actual IP address of the Syslog firewall and *level-name* is the severity level of the log

*Note: You must enter the set log command once for each message level.*

*The options for* ***level-name*** *are listed below:*

**emergency**

**alert**

**critical**

**error**

**warning**

**notification**

**information**

**debugging**

### Events to be Logged

The system logs contain historic firewall events and usage information, used for debugging system malfunctions and forensic investigations. Hence, log all critical information. Configure syslog to log the following on each firewall:

- Each login and logoff
- Firewall start-up and shutdown
- Complete session
- User and group account administration
- Hardware failures

### Log Retention and Archival

Many a times it is required to get a complete audit trail of a process for security investigation or troubleshooting purpose. Hence, locally retain the firewall logs for a defined number of days. There should be enough storage space allotted to handle this. In addition, there must be very strict access control implemented on the stored logs.

The log files must be archived offline. Appropriately protect the archived logs so that unauthorized users do not access them.

### Protection of Log Files

If a malicious user manages to modify the log files and remove traces of attack, no investigation can be conclusive. In addition, the log extended periods for audit trail. Hence, protect log files against tampering and stored securely.

### Session Activity Logs for Privileged Users

Privileged users have total control over the firewall. Log every activity performed on the firewall by these users.

### Periodic Monitoring

For maintaining the security levels on the Juniper firewalls, monitor the firewalls on a regular basis. Perform these monitoring tasks on periodic basis.

## Configuring Audit Loss Mitigation

There are cases where more auditable events can occur than the security appliance is able to write to a syslog firewall. The security appliance must stop further auditable events from occurring until the audit trail is able to handle more traffic. An authorized administrator must enable the following command:

**set log audit-loss-mitigation**

### Logging Permitted Packets

To log permitted packets passing through the device enable logging option on all authenticated and/or unauthenticated traffic policies.

In this document, all permitted policies include the keyword **log**, to create traffic log entries for permitted traffic.

Upon completion of the application session permitted traffic logs are created.

You can use the following command to view the overall traffic logs, or specific policy's traffic log:

**get log traffic**

**get log traffic policy** *id*

### Logging Dropped Packets

To log dropped packets set to terminate on any of the device interfaces, you must enable the following command:

**set firewall log-self**

To log authenticated dropped packets; you must add the **log** keyword to the first policy associated with a VPN tunnel. Packets that do not match any of the policies associated with the tunnel are "dropped". The log entries for these dropped packets linked with the highest priority policy (first in the '**get policy all**' list) associated with the tunnel and the traffic flow direction.

## Firewall Management Idle Timeout

### Command Line Interface

Protect Management from the console port by setting an idle timeout. By default, console and Telnet sessions time out after 10 minutes of inactivity. Recommend never to set the timeout value to zero.

To verify execute the command:

***get console***

### Web User Interface (WebUI)

The WebUI timeout, like the console timeout, defaults to 10 minutes. When changing the WebUI timeout, specify a number of minutes (between 1 and 999) of idle time before closing the browser. Enable the option “Enable Web Management Idle Timeout” check box. Do not disable it.

Security Manager

Edit Device > Device Admin > Web Management

### Permitted IP Addresses

Configure Juniper Networks devices to accept management requests only from trusted sources. Define a list of permitted IP addresses. Permitted IP addresses include a mask parameter specified as dotted-decimal value. Permitted IP addresses can be a hosts / subnets. NOTE: You are limited to six entries.

CLI

**set admin manager-ip address [mask]**

WebUI

Configuration >Admin > Permitted IPs

Security Manager

Edit Device > Device Admin > Permitted IPs > Add

### Daily Monitoring Tasks

- Three or more consecutive failed login attempts
- Syslog events with levels – critical, alert or emergency
- Unauthorized addition and deletion to user accounts and groups
- Changes / Unauthorized changes made
- Unauthorized access attempts

### Weekly Monitoring Tasks

- Correct operation of syslog daemon
- All resource (CPU, memory) usage exceeding pre-defined thresholds (based on capacity planning figures)

### Monthly Monitoring Tasks

- Firewall patch levels
- Firewall reboots
- Disk space usage
- Account group membership changes
- Verification of backups

### Bi Yearly Monitoring Tasks

- Perform Physical audit

The Juniper Firewall administrators must perform these monitoring tasks. Notify any discrepancy observed from normal operation to the appropriate department.

## FIREWALL PROTECTION

### Disaster Recovery Plan (DRP)

In order to provide protection against system failures, there has to be a tested and approved DRP. This should include the backup policy and contingency arrangements.

The DRP for each Juniper Firewall must be ready at the time the firewall is in production environment.

There must be a planned and bi-yearly Disaster Recovery Drill to ensure that the DRP is maintained and updated.

### Physical Security of Juniper Firewall installation

Physical security deals with all the security aspects of the installation premises of the actual firewalls

- Secure the physical location of the Juniper firewalls to guarantee operational continuity, protection against natural and fabricated disasters, and prevent loss of Information Assets.

- The Juniper firewalls must have uninterrupted and clean power supply, and operating conditions as recommended by the hardware vendors.

### Fault Tolerance

To ensure that failure of one firewall does not halt operations, each Juniper Firewall must use NSRP / HA for redundancy.

### Backup

Ensure that in case of data failure, manipulation or data loss; restore the system operations to previous working state at the earliest.

- Backup the data on each firewall using the standard operations procedures, to ensure that in case of failure, data recovery must conform to the SLA with the Business.
- Proper media labeling and protection should be implemented to ensure that media is not accidentally or deliberately overwritten.
- Verify the backup regularly by doing random restoration checks.
- The storage and retention of the computer media must be as per the manufacturer's recommendations.
- On expiry, the media should be disposed securely, ensuring no data extraction is possible

### Separation of test and Production environment

The test and development environment is usually set up with loose security controls. In order to avoid this, separate the Juniper Production firewalls from the test and development setup.

Irrespective of the settings and controls applied on test and development firewalls, the production firewalls must be hardened as per the Juniper Firewall security standards.

Do not create test user accounts on the Production firewalls.

There should be secure connection from test to Production firewalls.

Do not use data passing from production to the test environment without desensitizing it.

### Change Management

The Juniper firewalls must also adhere to this CM policy. The system administrators must ensure that every change goes through the appropriate CM process.

### Service Level Agreements for Screen OS and hardware support

For continuity of operation, protect the firewalls from extended downtimes due to Screen OS malfunctioning or hardware failure.

Each Juniper Firewall must have an SLA for Screen OS support (patches, troubleshooting etc) from an authorized Juniper Firewall vendor. Ensure that the firewalls are also be supported by an SLA with respective product vendors.

### Protection of firewalls not kept in the Data Center

Not all Juniper firewalls are located at the Data Center. Many of them are deployed in remote sites are housed in other locations with lesser protection – like the Lab \ Outstations. Hence, the respective teams must ensure that such firewalls have adequate access control and physical protection implemented.

### Documentation

The system administration and operations team must have complete documentation of the Juniper Firewall setup. This must include (but not limited to):

- Installation procedure
- Security settings
- Operating procedures
- Firewall configurations for each firewall
- Details of users for each firewall, with access rights
- Disaster Recovery Procedures for each firewall
- Regularly update the documentation.