|  |  |
| --- | --- |
|  |  |
|  |  |
|  | **Juniper ScreenOS Build Standard**  **V0.1** |
|  |  |
|  | **CONFIDENTIAL INFORMATION**  **This document is the property of Kaplan International; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Kaplan International.** |

Document Authorisation

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Date | Signature |
|  |  |  |  |

Document Review and Change History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Status | Issue Date | Next review date | Author Name | Description |
| 0.1 | Draft | N/A |  | Jamie Rose | Initial Draft |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

Document Authorisation 2

1 Introduction 5

1.1 Standard Owner 5

1.2 Scope 5

1.3 Related documents 5

1.4 Compliance 5

1.5 Sanctions 5

1.6 Exception process 6

2 The Standard 7

2.1 Accessing the device 7

2.1.1 Using a Console Connection 7

2.1.2 Using the WebUI 8

2.2 Upgrading to the Latest Firmware 8

2.2.1 Downloading New Firmware 8

2.2.2 Upgrading to the New Firmware 9

2.3 High Availability Configuration 11

2.3.1 Configuring HA Ports 12

2.3.2 Default Administrator Name and Password Change 13

2.3.3 Create Individual Administrator Accounts 13

2.3.4 Hostname and Domain Name 14

2.3.5 Login Banner 15

2.3.6 Creating a Login Banner Example 15

2.3.7 Domain Name System Server 16

2.3.8 Date and Time via Network Time Protocol (NTP) 17

2.4 Verifying External Connectivity 18

2.5 Restarting the Device 18

2.6 Creating New Security Zones 19

2.7 New Interface Creation 20

2.8 Management Settings – Manage-IP 20

2.9 Management Settings – SSH and SCP 20

2.10 Management Settings – HTTPS / SSL 21

2.11 Management Settings – NSM Express 22

2.12 Management Settings – SNMP 22

2.13 Authentication Settings 22

2.14 NAT Settings 23

2.15 Logging Configuration 23

2.16 Firewall Features – Intrusion Detection / Scanning configuration 24

2.17 Firewall Features – DoS Protection 24

2.18 Firewall Features – Deep Inspection 25

2.19 Firewall Features – Anti-Spoofing Protection 26

2.20 Firewall Features – OS Specific Attacks 26

2.21 Policy Settings – Comments and Deny All Logging 27

2.22 Device Settings – Default Route 27

|  |  |
| --- | --- |
|  |  |

1. Introduction

This standard has been created to assist in the deployment of a secure and consistent Juniper Networks Firewall ScreenOS build. The standard will outline the tasks needed to configure the Firewall with a set of baseline security requirements and functionality. This standard has been developed in line with the Kaplan Information Security Policy and the Kaplan Firewall and Switch Standard, please read both of these documents before proceeding.

* 1. Standard Owner

This standard is owned and distributed by the IT Operations Director

* 1. Scope

This standard applies to all Juniper Network firewalls within Kaplan, which protect system components that store, process, or transmit Cardholder Data (CHD) or Sensitive Authentication Data (SAD) and systems/segments that directly attach or support cardholder processing, storage, or transmission. This is commonly known as the Cardholder Data Environment (CDE). However, this procedure is equally relevant as a guideline for other Juniper firewalls within the Kaplan infrastructure.

* 1. Related documents
* The Kaplan Information Security Policy
* The Kaplan Firewall and Switch Standard
  1. Compliance

The Standard laid out in this document has been written to comply with various security standards, including ISO27001, ISF Standards of Good Practice and the Payment Card Industry Data Security Standard (PCI DSS). In addition to this Standard it should be noted that all Kaplan businesses must comply with the relevant local legislation. In the unlikely event that a Kaplan Standard conflicts with legislation, then that law must take precedence.

* 1. Sanctions

Instances of non-compliance with this procedure shall be identified, documented and escalated to the PCI Business owner. Deliberate non-compliance by individuals, whether they are system administrators or other users, shall be treated as a disciplinary offence.

* 1. Exception process

All exceptions to this Standard must be documented and managed via the *Kaplan Information Security Exception process*. Please contact the Information Security Manager for guidance.

1. The Standard
   1. Accessing the device

There are a number of ways to access the device, but for this build we will provide instructions how to issue actions via the web UI or via command line. Therefore, we will only show how to connect via the console port and the WebUI.

* + 1. Using a Console Connection

To establish a console connection with the device:

**N.B use a straight-through RJ-45 CAT5 cable with a male RJ-45 connector to plug into the Console port on the device.**

1. Plug the female end of the supplied DB-9 adapter into the serial port of your workstation. (Be sure that the DB-9 is inserted properly and secured.)
2. Plug one end of the RJ-45 CAT5 cable into the DB-9 adapter.
3. Plug the other end of the RJ-45 CAT5 cable into the Console port on the

ISG 1000-series device. Figure 2 shows the arrangement of the cable and adapter.



1. Launch a serial terminal-emulation program on your workstation, HyperTerminal for example. The required settings to launch a console session are as follows:
   * Baud rate: 9600
   * Parity: None
   * Data bits: 8
   * Stop bit: 1
   * Flow Control: None
2. Enter netscreen at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.). You will be instructed to change the default username and password as you first task on page 4

By default, the console times out and terminates automatically after

10 minutes of idle time. Please leave this setting in place.

1. Once the command prompt is displayed, the device is ready to be configured.
   * 1. Using the WebUI

To use the WebUI, the workstation from which you are managing the device must initially be on the same sub network as the device. To access the device with the

WebUI:

1. Connect your workstation to the port labeled **0/0** (ethernet0/0 interface), which is prebound to the Trust security zone.
2. Ensure that your workstation is configured with a static IP address in the 192.168.1.0/24 subnet.
3. Launch your browser, enter the IP address for the ethernet0/0 interface (the default IP address is 192.168.1.1), then press Enter.

The WebUI application displays the login prompt.

1. Enter netscreen at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.). You will be instructed to change the default username and password as you first task on page 4.
2. Once the WebUI homepage opens, the device is ready to be configured
   1. Upgrading to the Latest Firmware
      1. Downloading New Firmware

You can obtain the ScreenOS firmware from the Juniper Networks website. To access firmware downloads, you must be a registered customer with an active user ID and password. If you have not yet registered your Juniper Networks product, then you must do so at the Juniper Networks website before proceeding.

To get the latest ScreenOS firmware:

Navigate your browser to http://www.juniper.net/customers/support/. The

Support page appears.

1. Locate the DOWNLOAD SOFTWARE section, and click **ScreenOS**. Enter your user ID and password in the LOGIN page that appears, and then click the **LOGIN** button. The ScreenOS page appears.
2. In the table of software download versions, locate the device for which you want to download software and click the version you want.
3. In the Software tab (under Package), click the upgrade link. For some devices, you need to click the management module link before you can access the Software tab.
4. Click **Save**, then navigate to the location where you want to save the firmware zip file.

**N.B you must save the firmware onto the computer from which you want to perform the upgrade**.

* + 1. Upgrading to the New Firmware

This section provides instructions for upgrading firmware on the security device

using the WebUI, If you wish to upgrade via the CLI then please follow the instructions on page 20 of the Juniper ScreenOS 6.1 Upgrade Guide.

**N.B before upgrading a security device, save the existing configuration file to**

**avoid losing any data.**

This section describes how to upgrade the firmware on the security device using the

WebUI. Instructions include upgrading to an intermediate version of firmware, if

required, and then upgrading to ScreenOS 6.1.0.

To upgrade firmware using the WebUI:

1. Log into the security device by opening a browser.
2. Enter the management IP address in the Address field.
3. Log in as an admin with read-write privileges.

Save the existing configuration.

1. Go to **Configuration > Update > Config File**, and then click **Save To File**.
2. The File Download dialog box appears.
3. Click **Save**.
4. Navigate to the location where you want to save the configuration file

(cfg.txt), and then click **Save**.

Upgrade to the new ScreenOS firmware.

1. Go to **Configuration > Update > ScreenOS/Keys**, and then select **Firmware Update**.
2. Click **Browse** to navigate to the location of the new ScreenOS firmware, or enter the path to its location in the Load File field.
3. Click **Apply**. A message box appears with information on the upgrade time.
4. Click **OK** to continue. The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.
5. Log into the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI page.

**N.B this process takes some time. Do not click Cancel or the upgrade will fail. If you**

**do click Cancel and the upgrade fails, power off the device, then power it on**

**again. Restart the upgrade procedure beginning with Step 3.**

* + 1. Default Administrator Name and Password Change

The root administrative user has complete privileges to configure a device and is the only user able to create, modify or remove other admin users. Therefore, the default admin name (netscreen) and password (netscreen) must be changed immediately, used to create all the individual administrators and then locked away in the safe place in a tamper proof envelope and only used as part of the *Kaplan Break Glass Procedure*.

**N.B the root administrator password should be generated using a random password generator, e.g. PWGen, and must adhere to the Kaplan password policy as outlined in the Kaplan Information Security Policy on page 13**

To change the admin name and password:

**WebUI**

Configuration > Admin > Administrators > Edit (for the NetScreen

Administrator Name): Enter the following, then click **OK**:

Administrator Name:

Old Password: netscreen

New Password:

Confirm New Password:

**CLI**

set admin name *name*

set admin password *pswd\_str*

save

* + 1. Create Individual Administrator Accounts

To ensure that the root administrator account and password are locked away and only used in emergencies, we need to create individual read/write administrator accounts for all administrators of the Firewall. A full list of the current administrators of the Kaplan Juniper Firewalls can be found in Appendix A. Also, a full description of the levels of administration and roles can be found on page 415 of the *Juniper Networks Concepts & Examples**ScreenOS Reference Guide*

**N.B the individual administrator accounts passwords must adhere to the Kaplan password policy as outlined in the Kaplan Information Security Policy on page 13**

To create an individual read/write administrator account:

**WebUI**

Configuration > Admin > Administrators > New: Enter the following, then

click **OK**:

Name: Joe Bloggs

New Password: 2bd21wG7

Confirm New Password: 2bd21wG7

Privileges: Read-Write (select)

Role: None (default)

**CLI**

set admin user Joe Bloggs password 2bd21wG7 privilege read-write

save

* + 1. Hostname and Domain Name

The domain name defines the network or sub-network that the device belongs to, while the hostname refers to a specific device. The hostname and domain name together uniquely identify a device in the network. To configure the hostname and domain name on the device:

**WebUI**

Network > DNS > Host: Enter the following, then click **Apply**:

Host Name: *hostname*

Domain Name: *domain-name*

**CLI**

set hostname *hostname*

set domain *domain-name*

save

**N.B The naming convention for Kaplan is as follows:**

***THIS NEEDS TO BE DOCUMENTED***

* + 1. Login Banner

The login banner is a clear text ASCII file you create and store on the

security device, the file must be called **usrterms.txt**. Once copied to the firewall, the banner is activated by restarting the system. If the banner file is greater than 4Kbytes, the security device will not accept it and will continue using existing banners entered through the CLI and the WebUI.

When activated, the login banner is used globally by the root system and all virtual

systems (vsys). You cannot differentiate or customize between or within a vsys. The

login banner pre-empts all individually defined administrative access banners and

firewall authentication banners. After entering a username and password, the user

must click the **Login** button. Pressing the **Enter** key will not log the user into the

device.

* + 1. Creating a Login Banner Example

Use the SCP utility to securely copy the banner file to the security device. With the

following command, an administrator with copies the banner file **my\_large\_banner.txt** to a security device at IP address 1.1.1.2. The banner file must be saved on the security device as **usrterms.txt**.

linux:~#scp my\_large\_banner.txt netscreen@1.1.1.2:useterms.txt

You must restart the device to activate the new banner. To modify the banner file,

create a new file and overwrite the existing one with the new one.

***HERE IS A SAMPLE LOGIN BANNER – BANNER SHOULD BE AGREED BY KAPLAN BEFORE UPLOADING TO THE DEVICES***

*NOTICE TO USERS*

*THIS IS A PRIVATE COMPUTER SYSTEM. It is for authorized use only.*

*Users (authorized or unauthorized) have no explicit or implicit*

*expectation of privacy.*

*Any or all uses of this system and all files on this system may*

*be intercepted, monitored, recorded, copied, audited, inspected,*

*and disclosed to authorized site and law enforcement personnel,*

*as well as authorized officials of other agencies, both domestic*

*and foreign. By using this system, the user consents to such*

*interception, monitoring, recording, copying, auditing, inspection,*

*and disclosure at the discretion of authorized site personnel.*

*Unauthorized or improper use of this system may result in*

*administrative disciplinary action and civil and criminal penalties.*

*By continuing to use this system you indicate your awareness of and*

*consent to these terms and conditions of use. LOG OFF IMMEDIATELY*

*if you do not agree to the conditions stated in this warning.*

* + 1. Domain Name System Server

The Domain Name System (DNS) server on the network maintains a database for

resolving hostnames and IP addresses. Devices access the configured DNS servers

to resolve hostnames. In ScreenOS, you configure the IP addresses for the primary

and secondary DNS servers and the time of the day at which the device performs a

DNS refresh operation.

To configure the DNS server IP address and refresh time:

**WebUI**

Network > DNS > Host: Enter the following, then click **Apply**:

Primary DNS Server:  ***X.X.X.X***

Secondary DNS Server: ***X.X.X.X***

DNS Refresh: (select)

Every Day at: *time*

**CLI**

set dns host ***X.X.X.X***

set dns host ***X.X.X.X***

set dns host schedule *time*

save

* + 1. Date and Time via Network Time Protocol (NTP)

You can configure up to three NTP servers on a Juniper Networks security device:

one primary server and two backup servers. When you configure the security

device to synchronize its system clock automatically, it queries each configured NTP

server sequentially. The device always queries the primary NTP server first. If the

query is not successful, the device then queries the first backup NTP server and so

on until it gets a valid reply from one of the NTP servers configured on the device.

The device makes four attempts on each NTP server before it terminates the update

and logs the failure.

The security device sends NTP requests from a source interface and optionally uses

an encrypted, preshared key when sending NTP requests to the NTP server. The key

provides authentication.

**N.B the pre-shared key should generated using a random password generator, e.g. PWGen, and must adhere to the Kaplan password policy as outlined in the Kaplan Information Security Policy on page 13**

**WebUI**

Configuration > Date/Time: Enter the following, then click **Apply**:

Primary Server IP/Name: 1 ***X.X.X.X***

Primary server Key ID: 10

Source interface: Select Trust from the list.

Preshared Key: !2005abc *(Example only, please generate pre-sharedkey as instructed above)*

Backup Server1 IP/Name: ***X.X.X.X***

Primary server Key ID: 10

Source interface: Select Trust from the list.

Preshared Key: !2005abc

Backup Server2 IP/Name: ***X.X.X.X***

Primary server Key ID: 10

Source interface: Select Trust from the list.

Preshared Key: !2005abc

**CLI**

set ntp server ***X.X.X.X***

set ntp server backup1 ***X.X.X.X***

set ntp server backup2 ***X.X.X.X***

set ntp server src-interface trust

set ntp server backup1 src-interface trust

set ntp server backup2 src-interface trust

set ntp server key-id 10 pre-share-key !2005abc *(Example only, please generate pre-sharedkey as instructed above)*

set ntp server backup1 key-id 10 pre-share-key !2005abc

set ntp server backup2 key-id 10 pre-share-key !2005abc

save

* 1. Verifying External Connectivity

To verify that workstations in your network can access resources on the Internet,

start a browser from any workstation in the network and browse to [www.juniper.net/](http://www.juniper.net/)

* 1. Restarting the Device

You may need to restart the device in order to implement new features, such as

when you change between route and transparent mode or when you add new

license keys.

**CLI**

To restart the device with the CLI reset command:

* 1. Establish a console session with the device as described in *7.3.1* ***Using Console Connection*** on page 3.
  2. The device displays the login prompt
  3. Input your username and password
  4. At the console prompt, enter: **reset**
  5. The device prompts you to confirm the reset: **System reset, are you sure? y/[n]**

Enter **Y**.

* 1. The device restarts.

**WebUI**

To restart the device with the WebUI:

1. Launch your browser and enter the IP address for the management interface

(the default IP address is **192.168.1.1**), then press **Enter**.

The WebUI application displays the login prompt.

2. Input your username and password

3. In the WebUI, choose: **Configuration > Update > ScreenOS/Keys**

4. Click **Reset**.

An alert box prompts you to confirm that you want to reset the device.

5. Click **OK**.

The device resets. Also, an alert box prompts you to leave your browser open for a few minutes and then log back into the device.

* 1. Creating New Security Zones

By default all Juniper firewalls come with 3 predefined security zones: Trust, Untrust and DMZ. To add an additional DMZ, or to create a zone with your own name rather than use the default created zones, you must create the zone, assign it to a virtual router (VR) and then bind physical or logical interfaces to it.

**set zone name SHARED**  Creates the new zone called SHARED

**set zone SHARED vrouter trust-vr**  Binds the zone to trust-vr (default for all Kaplan FWs)

**set interface [PHYS\_IF] zone SHARED** Binds a physical interface to the new zone

* 1. New Interface Creation

The above example shows how to bind a physical address to a new security zone. To create a logical (i.e. VLAN) subinterface and bind it to a new zone:

**Set interface [PHYS\_IF].[VLAN\_ID] zone PCI**

**Set interface [PHYS\_IF].[VLAN\_ID] ip *X.X.X.X* 24 tag [VLAN\_ID]**

So, to create a subinterface using VLAN 100 and physical interface E1/1, the command would be:

**Set interface e1/1.100 zone PCI**

**Set interface e1/1.100 ip *X.X.X.X* /24 tag 100**

All interfaces should be configured in Route mode rather than NAT:

**Set interface e1/1.100 route**

* 1. Management Settings – Manage-IP

Given that the firewall will commonly be the default gateway address on a given network, you may not want the interface IP address to be the address that administrators actually use to connect to the device. This can be changed to a different address on the same subnet as the interface address.

**Set interface [IF] manage-ip [IP\_ADDRESS]**

So in the above example, if the IP address of the interface is 10.1.64.1, we might want administrators to connect to 10.1.6.254 instead:

**Set interface e1/1.100 manage-ip 10.1.64.254**

* 1. Management Settings – SSH and SCP

To access the CLI SSH should always be used as it is encrypted, and telnet should be disabled:

**Set ssh version v2**

**Set ssh enable**

**Set interface [IF] manage ssh**

Disable Telnet from all interfaces:

**Unset interface e0 manage telnet**

**Unset interface e1 manage telnet**

**Unset interface e2 manage telnet**

Optionally, you can change the default SSH port from port 22 to something else:

**Set admin ssh port 2222**

SCP is a secure file transfer utility that uses SSH as its underlying transport, and it should be used for transferring firmware files, certificates, logs and banners to and from the firewall. To enable it:

**Set scp enable**

* 1. Management Settings – HTTPS / SSL

When using the web GUI, ensure that it always uses SSL encryption, and that attempts to connect via HTTP are redirected to HTTPS. As with SSH, optionally a non-standard port number can be used for HTTPS – in this example port 8443 is used rather than 443:

**Set ssl port 8443**

**Set ssl cert 1**

**Set ssl encrypt 3des**

**Set ssl enable**

Now that SSL is enabled, you must configure the interfaces through which you want to connect to the device to administer it:

**Set interface e2 manage ssl**

To enable the redirection of HTTP request to HTTPS, use the following command:

**Set admin http redirect**

* 1. Management Settings – NSM Express

The firewalls may be managed via SNMP, Netscreen Security Manager or both. To enable NSM:

**Set nsmgmt server primary [IP\_ADDRESS]**

After setting the server IP address, configure the firewall to send remote logs and alarms to the management platform:

**set nsmgmt report statistics attack enable**

**set nsmgmt report statistics policy enable**

**set nsmgmt report alarm attack enable**

**set nsmgmt report alarm traffic enable**

**set nsmgmt report statistics traffic enable**

**set nsmgmt report statistics flow enable**

**set nsmgmt report alarm idp enable**

**set nsmgmt report alarm other enable**

Now, enable NMS Management on the actual interface connecting back to the central manager:

**set interface e2 manage nsmgmt**

* 1. Management Settings – SNMP

At the time of writing the assumption is that SNMP will not be used to manage the firewalls. To disable SNMP management on all interfaces:

**unset interface [IF] manage snmp**

* 1. Authentication Settings

**THIS NEEDS TO BE DEFINED. WHAT AUTHENTICATION METHOD DO WE USE FOR THE JUNIPER FIREWALLS TACACS+ or RADIUS?**

* 1. NAT Settings

Juniper firewalls have the ability to create interfaces in NAT mode, where all traffic passing through that interface is Port Address Translated (PAT) behind the address of the interface. While it seems like a quick and easy way to deploy internet connectivity, routed mode with policy-based NAT is much more flexible and should be enabled on all interfaces:

**Set interface [IF] route**

To perform PAT (1:many NAT), create a DIP (Dynamic IP) pool of addresses to be natted against:

**Set interface [IF] dip [DIP ID] [START\_IP\_ADDRESS] [END\_IP\_ADDRESS]**

So to create a pool of 5 addresses for dynamic translation on Ethernet 1 called DIP ID 5:

**Set interface ethernet1 dip 5 *X.X.X.X***

To then use that pool of dynamic addresses, it should be referenced in the actual firewall policy. So in this example, to hide HTTP traffic behind one of those dynamic IP addresses you would type:

**Set policy from trust to PCI any any http nat src dip-id 5 permit log**

* 1. Logging Configuration

The Juniper firewalls can output system alerts, attack alarms and general traffic logs via standard syslog. Logs and Alerts should be sent to an external logging server as follows:

**Set syslog config *X.X.X.X* port 514**

**Set syslog config *X.X.X.X* all**

**Set syslog config *X.X.X.X* facilities local0 local0**

Optionally (if your syslog appliance supports it) transport can be sent over TCP rather than UDP to ensure session reliability:

**Set syslog config *X.X.X.X* transport tcp**

* 1. Firewall Features – Intrusion Detection / Scanning configuration

The Juniper firewalls are capable of detecting many typical information-gathering activities that are generally performed as a precursor to any intrusion attempt, such as OS fingerprinting and general port scans and ping sweeps.

The following configuration should be applied to all external facing interfaces – that is, the untrust zone of network boundaries such as the Internet firewalls. It will be less necessary on the Untrust interfaces of the newly deployed PCI desk firewalls as they are not boundaries between the LAN and Internet or other untrusted parties:

**set zone untrust screen ip-sweep threshold 1000  
set zone untrust screen ip-sweep  
set zone untrust screen port-scan threshold 100  
set zone untrust screen port-scan  
set zone untrust screen tcp-sweep  
set zone untrust screen udp-sweep  
set zone untrust screen ip-record-route  
set zone untrust screen ip-timestamp-opt  
set zone untrust screen ip-security-opt  
set zone untrust screen ip-stream-opt  
set zone untrust screen syn-fin  
set zone untrust screen fin-no-ack  
set zone untrust screen tcp-no-flag  
set zone untrust screen fin-no-ack,  
set flow tcp-syn-check.**

* 1. Firewall Features – DoS Protection

The most common type of attack against internet-connected hosts is a simple Denial Of Service attack, which despite its simplicity can successfully cripple almost ay target. While protecting against a DoS attack usually involves working with your ISP to throttle the attack closer to the source, the Juniper firewalls have a range of settings that can themselves choke potential disruptive hosts when attempting to pass through the firewall.

Again, these settings should be configured on the internet-facing zones only.

**set zone untrust screen limit-session destination-ip-based 4000  
set zone untrust screen limit-session destination-ip-based**

**set zone untrust screen syn-ack-ack-proxy threshold 500  
set zone untrust screen syn-ack-ack-proxy  
set zone untrust screen syn-flood  
set zone untrust screen syn-flood attack-threshold 2000  
set zone untrust screen syn-flood alarm-threshold 1000  
set zone untrust screen syn-flood source-threshold 250  
set zone untrust screen syn-flood destination-threshold 250  
set zone untrust screen syn-flood timeout 20  
set zone untrust screen syn-flood queue-size 1000  
set zone untrust screen syn-flood  
set zone untrust screen icmp-flood threshold 100  
set zone untrust screen icmp-flood  
set zone untrust screen udp-flood threshold 1000  
set zone untrust screen udp-flood**

* 1. Firewall Features – Deep Inspection

Juniper firewalls have in-built signatures of various common attacks on protocols such as HTTP, FTP, DNS etc. Deep inspection goes above normal layer 4 (port and protocol) inspection, and instead recognises the underlying protocol used, and understands what are normal and valid requests and uses of that protocol. By enabling Deep Inspection on commonly used protocols, the firewall can see inside the actual packets and determine if a particular session is behaving maliciously or unusually.

Deep inspection should be enabled on all policies that have a valid application signature pack. In the Kaplan network this means HTTP, HTTPS/ SSL, SSH and SMTP inbound from the external mail relays.

Deep inspection is enabled at the command line via the ATTACK keyword after the policy permit statement. As you will often want to apply multiple deep inspection rules to a single policy, it is useful to enter policy configuration mode. In the following example, a policy with an ID number 1 is created, permitting HTTP traffic from the LAN to the DMZ:

**Set policy id 1 from trust to untrust permit 192.168.1.0/24 any http permit “Internet access” log**

To make further changes to this policy entry, type

**Set policy id 1**

You will see the prompt change to

**Hostname(policy:1)->**

This means you are now in policy editing mode. You can now change the source, destination, protocols and actions associated with that policy.

To enable HTTP inspection of critical signature attacks, type:

**Set attack CRITICAL:HTTP:SIGS action close-server**

The format for deep inspection commands is

**THREAT\_LEVEL:PROTOCOL:INSPECTON\_TYPE**

Threat levels are Critical, High and Medium Low and Info.

Protocols are continually updated but include DNS, SMTP, HTTP, HTTPS, SSL, FTP and SSH.

Inspection types are SIGS for checking against known threat signatures, and ANOM for anomalous protocol inspection (i.e. unusual or malformed packets)

Deep inspection should not be applied by default to each and every policy – it consumes firewall resources, and if a HTTP inspection policy is applied to a group policy that contains traffic other than HTTP it will try to inspect every other flow, which wastes processing power. Instead, individual critical flows (such as HTTPS to DMZ servers, SMTP to inbound mail gateways, FTP to or from any server) should be subject to deep inspection.

* 1. Firewall Features – Anti-Spoofing Protection

Many network attacks rely on hiding (spoofing) the IP address of the attacker behind another invalid address. To protect against this, the firewall can enable anti-spoofing protection. Anti-spooding protection uses the firewalls routing table to decide whether a packet received on an interface has a valid source address. If a trust interface only has a route to 192.168.0.0/16 and it receives a packet from 10.10.10.1, it will drop it due to anti-spoofing rules.

Anti-spoofing should be enabled on all zones on the firewalls:

**set zone untrust screen ip-spoofing**

**set zone trust screen ip-spoofing**

**set zone dmz screen ip-spoofing**

* 1. Firewall Features – OS Specific Attacks

The Juniper firewalls can detect and protect against many (mostly historic) OS specific attacks such as Windows Nuke. LAND attacks etc. Screening against these attacks should be enabled on the untrust zone:

**set zone untrust screen land  
set zone untrust screen ping-death  
set zone untrust screen tear-drop  
set zone untrust screen winnuke**

* 1. Policy Settings – Comments and Deny All Logging

For PCI compliance to be maintained and for ease of firewall troubleshooting, it is important that all policy entries have a valid comment attached. This should reference the change record (if relevant) and/or provide justification for the flow that has been created.

Similarly, it is important that at the end of every policy from every zone to every other zone there is an explicit ‘drop all’ rule that is configured with logging enabled. This aids troubleshooting when tracing traffic logs, and can be a useful forensic tool in the event of security incident.

**Set policy from trust to untrust 10.1.0.0/20 any dip 5 permit “HTTP Internet Access CGHxxxx” log**

**Set policy from trust to untrust any any deny “Default Deny” log**

**Set policy from untrust to trust any any deny “Default Deny” log**

**Set policy from trust to dmz any any deny “Default Deny” log**

**Set policy from dmz to trust any any deny “Default Deny” log**

**Set policy from dmz to untrust any any deny “Default Deny” log**

**Set policy from untrust to dmz any any deny “Default Deny” log**

* 1. Device Settings – Default Route

Juniper firewalls by default have two in-built routers, the trust-vr and the untrust-vr. They can maintain individual routing tables, and can be used to ensure that packets entering from the internet (untrust) side of the firewall only ever have a route to particular DMZ hosts, while internal users can have a separate routing table.

In practice, most deployments only use the trust-vr, which by default is bound to all zones and interfaces.

The default route is a static route used to direct packets addressed to networks that

are not explicitly listed in the routing table. If a packet arrives at the device with an

address for which the device does not have routing information, the device sends

the packet to the destination specified by the default route. To configure the default route on the device:

**set route 0.0.0.0/0 interface untrust gateway [ISP\_ROUTER\_ADDRESS]**