Hardening Junos Devices Checklist

The companion checklist to *This Week: Hardening Junos Devices, Second Edition*

Date: _____ Device Name: _____ Location: _____ Rack/Row: _____

IP Address: _____ NetMask: _____ Gateway: _____ MAC: _____

Administrative (see Chapter 1)

- ☐ Research the latest Juniper Security Advisories
- ☐ Install recommended version of Junos: _____

Physical Security (see Chapter 2)

- ☐ If redeploying a previously installed device, perform a media installation to remove previous configurations and data

Secure Physical Ports

- ☐ Disable unused network ports

Console Port

- ☐ Configure the logout-on-disconnect feature
- ☐ Configure the insecure feature

Auxiliary Port

- ☐ Disable the Auxiliary port
- ☐ Configure the insecure feature

Diagnostic Ports

- ☐ Password protect Diagnostic ports

Craft Interface/LCD Menu

- ☐ Disable unnecessary functions for your environment

Network Security (see Chapters 3 & 4)

- ☐ Use the Out-of-Band (OOB) interface for all management related traffic (Ch. 3)
- ☐ Enable the default-address-selection option (Ch. 4). Set the source address for all route engine generated traffic (NTP, SNMP, Syslog, etc.)
- ☐ Globally disable ICMP redirects (Ch. 4)
- ☐ Ensure Source Routing has not been configured (Ch. 3)
- ☐ Ensure IP directed broadcast has not been configured (Ch. 3)
- ☐ Ensure Proxy ARP is either not configured, or is restricted to specific interfaces (Ch. 3)
- ☐ Drop TCP packets with the SYN and FIN flag combination (Ch. 4)
- ☐ Disable ICMP timestamp & record route requests (Ch. 4)
- ☐ Disable ICMP Source Quench
- ☐ Configure LLDP only on required network ports (Ch. 4)

Management Services Security (see Chapter 4)

- ☐ Configure NTP with authentication with more than one trusted server
- ☐ Configure SNMP using the most secure method with more than one trusted server
- ☐ Community strings and USM passwords should be difficult to guess and should follow a password complexity policy
- ☐ Configure read-only access; use read-write only when required
- ☐ Allow SNMP queries and/or send traps to more than one trusted server
- ☐ Send Syslog messages to more than one trusted server with enhanced timestamps
- ☐ Configure automated secure configuration backups to more than one trusted server

Access Security (see Chapter 4)

- ☐ Configure a warning banner that is displayed prior to login
- ☐ Disable insecure or unnecessary access services (telnet, J-Web over HTTP, FTP, etc.)
- ☐ Enable required secure access services:

SSH

- ☐ Use SSH version 2
- ☐ Deny Root logins
- ☐ Set connection-limit and rate-limit restrictions

J-Web

- ☐ Use HTTPS with a valid certificate signed by a trusted CA
- ☐ Limit access to only authorized interfaces
- ☐ Terminate idle connections by setting the idle-time value
- ☐ Set session-limit restrictions suitable for your environment

Continued on Page 2

User Authentication Security (see Chapter 4)

- ☐ Configure a password complexity policy
  - ☐ Minimum password length, upper case, lower case and special characters
  - ☐ Use SHA1 for password storage
- ☐ Ensure the root account has been configured with a strong password
- ☐ Configure login security options to hinder password guessing attacks
- ☐ Configure custom login classes to support engineers with different access levels using the least privilege principle
  - ☐ Restrict commands by job function
  - ☐ Set appropriate idle timeout values for all login classes
  - ☐ Limit access to ## SECRET-DATA

Centralized authentication

- ☐ Use a strong shared secret that complies with your organization's password complexity policy
- ☐ Configure multiple servers for resiliency
- ☐ Configure accounting to trace activity and usage
- ☐ Create an emergency local account in the event authentication servers are unavailable

Local Authentication

- ☐ Know the origin and purpose for all configured local accounts
- ☐ Limit local accounts to required users
- ☐ Use a strong password that complies with your organization's password complexity policy
- ☐ Set the authentication-order to meet your login security policy

Routing Protocol Security (see Chapter 4)

- ☐ Ensure routing protocols are only configured on required interfaces
- ☐ BGP communication should source from a loopback interface
- ☐ Configure route authentication with internal and external trusted sources
  - ☐ Select the strongest algorithm that is supported by your equipment and your neighbors
  - ☐ Use strong authentication keys that meet your organization's password complexity policy
  - ☐ Limit key exposure by using separate authentication keys for different organizations
- ☐ Periodically change route authentication keys in accordance with your organization's security policy (consider using hitless key rollover if the routing protocol supports it)

Firewall Filter (see Chapter 4)

- ☐ Protect the Routing Engine using a default deny firewall filter
- ☐ Order terms with time sensitive protocols at the top
- ☐ Permit only required protocols from authorized sources
- ☐ Rate-limit SYN packets to protect against a SYN flood attack
- ☐ Rate-limit authorized protocols using policers
- ☐ Ensure the last term, default-deny, includes the syslog option

Installer: _____ Installer Phone: _____ Installer Email: _____

Owner: _____ Owner Phone: _____ Owner Email: _____

This excerpt is from *This Week: Hardening Junos Devices, Second Edition*, available at http://www.juniper.net/dayone, and also available in eBook format on the iTunes Store>iBooks or the Amazon.com Kindle store.

THIS WEEK COMPANION

Hardening Junos Devices Checklist

Juniper Networks Information and Learning Experience (iLX)

www.juniper.net/posters