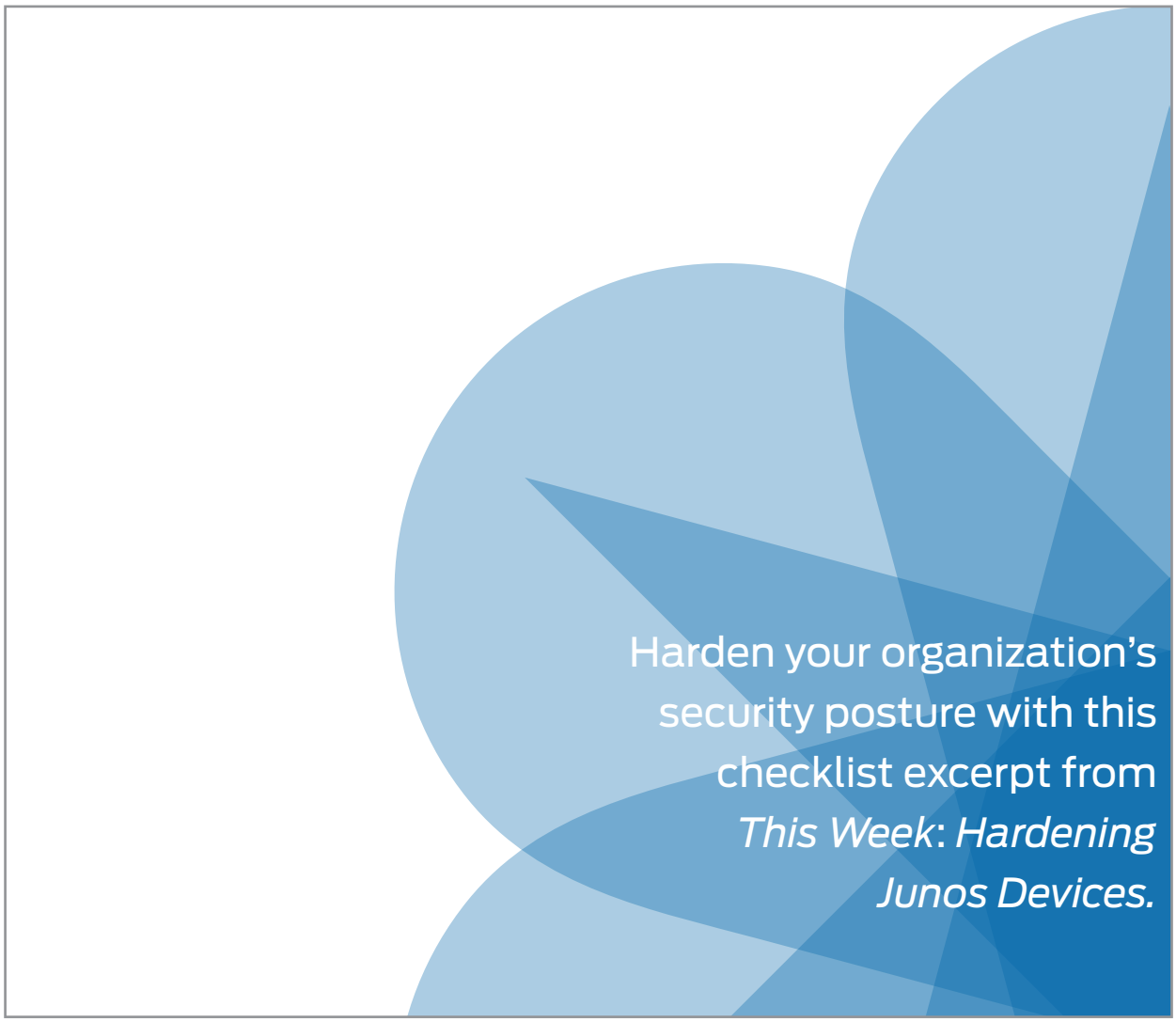
JUNIPER NETWORKS

A Junos® Fundamentals Excerpt

THIS WEEK: HARDENING JUNOS DEVICES CHECKLIST



By John Weidley

Administrative *(see Chapter 1)*

- Research the latest Juniper Security Advisories
- Install the latest supported/recommended version of Junos
- Always verify cryptographic checksums prior to installation

Physical Security *(see Chapter 2)*

- If you're redeploying a previously installed device, perform a media installation to ensure all previous configuration and data is removed
- Console Port
  - ☐ Configure the logout-on-disconnect feature
  - ☐ Configure the insecure feature
- Auxiliary Port
  - ☐ Disable the Auxiliary port if you don't have a valid use
  - ☐ Configure the insecure feature
- Diagnostic Ports
  - ☐ Set a strong password for Diagnostic ports
- Craft Interface/LCD Menu
  - ☐ Disable unnecessary functions for your environment
- Disable unused network ports

Network Security *(see Chapters 3 & 4)*

- Use the Out-of-Band (OOB) interface for all management related traffic (see Chapter 3)
- Enable the default-address-selection option (see Chapter 4)
  - ☐ Or, set the source address for all routing engine generated traffic (NTP, SNMP, Syslog, etc.)
- Globally disable ICMP redirects (see Chapter 4)
- Ensure Source Routing has not been configured (see Chapter 3)
- Ensure IP directed broadcast has not been configured (see Chapter 3)
- Ensure Proxy ARP is either not configured, or is restricted to specific interfaces (see Chapter 3)
- Configure the routing engine (RE) to drop TCP packets with the SYN & FIN flag combination (see Chapter 4)
- Configure the RE to hide lo0 IP address for ICMP timestamp & record route requests (see Chapter 4)
- Configure LLDP only on required network ports (see Chapter 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
  - ☐ Be sure to configure read-only access; use read-write only when absolutely required
  - ☐ Allow 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 credentials being provided
- 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 suitable for your environment
  - ☐ J-Web
    - ♦ Use HTTPS with a valid certificate signed by a trusted CA
    - ♦ Restrict access only from authorized particular interfaces
    - ♦ Terminate idle connections by setting the idle-time value
    - ♦ Set session-limit restrictions suitable for your environment

User Authentication Security *(see Chapter 4)*

- Configure a password complexity policy
  - ☐ Minimum password length, character-sets, and minimum changes
  - ☐ Use SHA1 for password storage
- Ensure the root account has been configured with a strong password that meets your organization's password complexity policy
- 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 reasonable idle timeout values for all login classes

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

Routing Protocol Security *(see Chapter 4)*

- Be sure routing protocols only 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 firewall filter with a default deny policy
  - ☐ Ensure to permit only required ICMP types and deny all other ICMP types and codes
  - ☐ Ensure the last term, default-deny, includes the syslog option so all denied traffic can be centrally monitored
- Rate-limit common protocols used in flooding attacks
- Rate-limit authorized protocols using policers (within reasonable limits)

MORE? This excerpt is from *This Week: Hardening Junos Devices* by John Weidley, available at http://www.juniper.net/dayone, and also available in eBook format on the iTunes Store>Books or the Amazon.com Kindle store.