Hardening Network Devices

Hardening network devices reduces the risk of unauthorized access into a network's infrastructure. Vulnerabilities in device management and configurations present weaknesses for a malicious cyber actor to exploit in order to gain presence and maintain persistence within a network. Adversaries have shifted their focus from exclusively exploiting traditional endpoints to increasingly exploiting specialized and embedded devices, including routers and switches. They do this through manipulating weaknesses in configurations, controlling routing protocols, and implanting malware in the operating systems.

Service Security Recommendations

All networking devices, including routers and switches, come equipped with services turned on when they are received from the manufacturer. Disabled services cannot be exploited by an adversary. Therefore, all unnecessary services should be disabled. By default, each manufacturer turns off different services in their standard out-of-the-box configuration, and default services may vary among operating systems. Research should be done to determine what services are running by default. The following guidance will serve to determine the services that should be enabled or disabled:

Enable

- **SSHv3 or TLS:** Both of these protocols are used to securely communicate to remote network devices.

Disable

- **Echo Protocol:** A legacy protocol to measure the round trip time of a packet.
- **Chargen Protocol:** A legacy protocol that uses arbitrary characters to test, debug, and measure the connection.
- **Discard Protocol:** A legacy protocol to simply discard received packets.
- **Daytime Protocols:** Returns ASCII character strings of the current date and time.
- **FTP Protocol**: Allows users to copy files between their local system and any system that can be reached on the network.
- **Telnet:** An application layer clear text protocol used on the network to communicate with another device.
- **BootP Service:** A legacy protocol used to assign an IP address to a device.
- **HTTP Server:** Most devices come with a Web service enabled by default.
- **SNMP Protocol:** A protocol to manage network devices. If needed, only run SNMPv3 with a Management Information Base (MIB) allow list ("Reducing the risk of Simple Network Management Protocol SNMP Abuse" [1]) and do not use SNMP community strings.
- **Discovery Protocols:** These protocols are used to share information with neighboring devices and discover the platform of those devices.
- **IP Source Routing:** Allows the sender to control the route of information to the destination.
- **IP Unreachable:** Internet Control Message Protocol (ICMP) messages can be used to map out the network

[1] https://apps.nsa.gov/iaarchive/library/ia-advisories-alerts/reducing-the-risk-of-snmp-abuse.cfm

topology.

- **IP Mask Reply:** Replies respond to ICMP mask requests by sending out ICMP mask replies containing important network information.
- **Zero Touch Provisioning:** Zero touch provisioning allows network devices to reach out to download firmware and configurations without any user interaction.

Interface and Switch Port Recommendations

As with services, all router interfaces and switch ports that are not used should be disabled to prevent unauthorized access to the device.

- Enable port security.
- Shut down unused interfaces and switch ports.
- Place unused switch ports in a VLAN that is not routed and closely monitored. Reassign the native VLAN.

Disable

- Unused interfaces and routing protocols
- IP direct-broadcast
- IP proxy-arp

Secure Access Recommendations

There are several ways to access network devices: through an administrative connection, console line, auxiliary line, and virtual terminal connection. Each method should be secured to prevent any unauthorized access to the network device. The following security configurations need to be implemented to limit and secure access to the router or switch from the console, auxiliary, and Virtual Teletype (VTY) ports:

- Use multi-factor authentication using hardware tokens and passwords.
- Use out-of-band management to separate network administration traffic from normal user traffic.
- Implement the manufacturer's configuration guidance to restrict access to the console port.
- Limit the number of simultaneous management connections.
- Enable the strongest password encryption supported by the equipment.
- Follow "Digital Identity Guidelines – Authentication and Lifecycle Management" (NIST SP 800-63B[2]).
- Reduce the risk of exposing administrative interfaces to user traffic by applying IP address access control lists.
- Restrict physical access to routers/switches and apply access control lists for remote access.
- Monitor and log all attempts to access network devices.

[2] https://pages.nist.gov/800-63-3/sp800-63b.html

Vendors of network infrastructure devices often provide detailed documentation with security guidance for each of their products. In addition to applying the above mitigations, it is also recommended to apply the security guidelines available through vendor publications.

General Security Recommendations

- Install the latest version of the network device's operating system and approved patches to protect from known vulnerabilities to the vendor's equipment.
- All updated patches should be tested before implementing them on the enterprise to ensure operational network stability and legacy applications continue to work.
- Create and enforce the Site Security Policy (SSP) to secure all devices. The SSP should outline roles and responsibilities to manage and monitor devices and services. Each role should only have the lowest privilege access that is required to perform required tasks.
- Back up configuration files and store them offline.
- Never share configuration files by using unsecure means, such as email, File Transfer Protocol (FTP), or publishing them to a website. This could allow an adversary to gain insight into the enterprise architecture or decrypt password hashes.
- Disable unused services and implement an access control list to protect services that are required by the SSP.
- Periodically test the security of the network devices and compare the configuration against the site SSP or original configuration to verify the configuration of all network equipment.
- Compare the offline hash of the operating system against the hash of the vendor's known good operating system image to validate the integrity.
- Safeguard configuration files with encryption and/or password protection when sending them electronically and when they are stored and backed up.

Disclaimer of Endorsement

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov