Router and Switch Security Policy

1.0 Purpose

Routers and switches form the backbone of the organization's network infrastructure. Their secure configuration is paramount to maintaining network integrity, availability, and protecting data traversing the network. This standard establishes the minimum required security configuration for all routers and switches connected to or operating within the organization's production network environment to mitigate risks associated with misconfiguration and unauthorized access.

2.0 Scope

This standard applies to all employees, contractors, consultants, temporary staff, vendors, and other personnel responsible for the configuration, management, or operation of routers and switches connected to the organization's production networks. It covers all such devices owned or managed by the organization.

3.0 Standard Requirements

All routers and switches within the scope of this standard must adhere to the following minimum security configuration requirements:

3.1 Authentication and Access Control

*   **Centralized Authentication:** Local user accounts must be disabled. All administrative authentication to routers and switches must utilize the organization's approved centralized authentication system (e.g., TACACS+, RADIUS) integrated with central identity stores.
*   **Enable/Privileged Mode Security:** Access to privileged ('enable') mode must be secured. The enable password/secret must be stored in a secure, encrypted format on the device and must comply with the organization's password complexity and management policies. Enable passwords should be managed centrally where possible and rotated regularly.
*   **Management Access Protocols:** Secure protocols must be used for administrative access. SSH version 2 is the required protocol for remote command-line access. Telnet is strictly prohibited unless tunnelled over a secure, encrypted connection (e.g., IPsec VPN).
*   **Access Control Lists (ACLs):** Infrastructure ACLs must be implemented to restrict management access (SSH, SNMP, NTP, TACACS+/RADIUS source IPs, etc.) to the device itself, permitting connections only from authorized management subnets or hosts.
*   **Console/Aux Port Security:** Physical console and auxiliary port access must be controlled through physical security measures and may require additional authentication controls.

3.2 Service Hardening

The following services and features must be **disabled** unless a specific, documented, and approved business justification exists:

* IP Directed Broadcasts
* TCP Small Services (echo, discard, chargen, daytime)
* UDP Small Services (echo, discard, chargen, daytime)
* IP Source Routing
* Proxy ARP (unless specifically required and approved)
* HTTP/HTTPS server (web interface) for device management (unless specifically approved with strong authentication and TLS)
* Telnet server
* FTP server
* Configuration Auto-loading features
* Vendor-specific discovery protocols (e.g., CDP, LLDP) on interfaces facing untrusted networks (e.g., Internet, external partners). May be disabled internally unless required for specific network functions (e.g., VoIP phone discovery).
* Dynamic Trunking Protocol (DTP) on switch ports (configure ports statically as access or trunk).
* Scripting environments (e.g., TCL shell) unless explicitly required for approved automation tasks.

3.3 Secure Configuration Settings

* **Password Encryption:** The service to encrypt passwords stored in the device configuration (e.g., `service password-encryption` or equivalent) must be enabled. (Note: This provides only obfuscation; stronger protection relies on secure authentication protocols and restricted configuration access).
* **Network Time Protocol (NTP):** Devices must be configured to synchronize their time with approved, redundant internal NTP sources traceable to a reliable external standard.
* **Simple Network Management Protocol (SNMP):**
  * If SNMP is used, default community strings (e.g., "public," "private") must be removed or changed to strong, complex values compliant with password policies.
  * SNMP access must be restricted using ACLs to authorized management stations only.
  * SNMPv3, which provides encryption and authentication, is the required version. Use of SNMPv1 or v2c requires a documented exception and strong justification.
* **Logging:** Devices must be configured to log security-relevant events (logins, configuration changes, ACL denials) to the organization's centralized logging system (SIEM) via secure syslog, adhering to the Audit Logging Policy.
* **Login Banner:** The following standard warning banner (or an organization-approved equivalent) must be configured and presented for all login attempts (console, SSH):
  > "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

3.4 Routing Security

*   **Secure Routing Updates:** Dynamic routing protocols (e.g., EIGRP, OSPF, BGP) must utilize neighbor authentication (e.g., using MD5 or SHA hashes with strong keys) for all routing updates. Password hashing features for the authentication string must be enabled where supported.
*   **Route Filtering:** Appropriate route filtering must be implemented to prevent injection of inappropriate routes.
*   **Anti-Spoofing:** Ingress filtering (e.g., Unicast Reverse Path Forwarding - uRPF, or ACLs) must be implemented on interfaces, particularly edge interfaces, to drop packets sourced with invalid or illegitimate addresses (e.g., RFC1918 addresses from the Internet, bogons, internal addresses arriving on external interfaces).

3.5 Sensitive Device Requirements

Certain critical routers and switches (e.g., core devices, perimeter firewalls/routers, devices handling highly sensitive data) may be designated as "sensitive" and require additional security controls as defined by the designated IT authority (e.g., Precision Computer). These may include:

*   More detailed logging configurations (e.g., IP ACL accounting).
*   Enhanced monitoring.
*   Stricter access controls and change management procedures.

3.6 Network Management Integration

*   All production routers and switches must be registered in the organization's network management and asset inventory systems with accurate configuration details and designated points of contact.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this standard through various methods, including automated configuration audits, vulnerability scanning, manual reviews, penetration testing, internal/external audits, and review of network monitoring data.

4.2 Exceptions

Any exception to this standard requires formal, documented justification outlining the technical necessity or constraint, risk assessment including compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

*   Devices found to be non-compliant with this standard must be remediated within a defined timeframe or risk being isolated or removed from the production network.

*   Failure by personnel responsible for device management to adhere to this standard may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

*   **Production Network:** The primary operational network infrastructure supporting the organization's core business functions and services.
*   **TACACS+ (Terminal Access Controller Access-Control System Plus):** A protocol providing centralized authentication, authorization, and accounting (AAA) for network device administration.
*   **RADIUS (Remote Authentication Dial-In User Service):** Another common protocol for centralized AAA.
*   **ACL (Access Control List):** A set of rules applied to network interfaces to permit or deny traffic based on criteria like source/destination IP address, port numbers, and protocols.
*   **SNMP (Simple Network Management Protocol):** A protocol used for monitoring and managing network devices. SNMPv3 adds security features.
*   **SSH (Secure Shell):** A cryptographic network protocol for operating network services securely over an unsecured network.
*   **NTP (Network Time Protocol):** A protocol for synchronizing the clocks of computer systems over packet-switched networks.
*   **RFC1918 Addresses:** Private IPv4 address ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) not routable on the public Internet.

6.0 Related Policies

*   Password Policy
*   Audit Logging Policy
*   Acceptable Use Policy
*   Change Management Policy
*   Vulnerability Management Policy
*   Information Security Policy (Overall)
*   Network Segmentation Policy / Architecture Documents

Revision #2
Created 28 August 2024 16:57:37 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery