Router and Switch Security Policy

1. Overview

See Purpose.

2. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of The Catholic Diocese of Columbus.

3. Scope

All employees, contractors, consultants, temporary and other workers at the Diocese and its subsidiaries must adhere to this policy. All routers and switches connected to Diocese production networks are affected.

4. Policy

Every router must meet the following configuration standards:

1. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
2. The following services or features must be disabled:
    a. IP directed broadcasts
    b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c. TCP small services
    d. UDP small services
    e. All source routing and switching
    f. All web services running on router
    g. Cisco discovery protocol on Internet connected interfaces
    h. Telnet, FTP, and HTTP services
    i. Auto-configuration
3. The following services should be disabled unless a business justification is provided:
    a. Cisco discovery protocol and other discovery protocols
    b. Dynamic trunking
    c. Scripting environments, such as the TCL shell
4. The following services must be configured:
    a. Password-encryption
    b. NTP configured to a corporate standard source
5. All routing updates shall be done using secure routing updates.

6. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
7. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
8. Access control lists for transiting the device are to be added as business needs arise.
9. The router must be included in the corporate enterprise management system with a designated point of contact.
10. Telnet may never be used across any network to manage a router unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
11. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
12. The corporate router configuration standard will define the category of sensitive routing and switching devices and require additional services or configuration on sensitive devices including:
    a. IP access list accounting
    b. Device logging
    c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    d. Router console and modem access must be restricted by additional security controls

5. Policy Compliance

5.1 Compliance Measurement

The Technical Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru's, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Technical Services team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies, and Processes

None.

7 Definitions and Terms

None.