Provo City School District Technology Security Policy

Router and Switch Security Procedure

Last Update Status: *Updated January 2015*

1. Purpose

The purpose of this procedure is to describe the minimal security configuration required for all routers and switches connecting to a production network or used in a production capacity at or on behalf of PCSD.

2. Scope

All employees, contractors, consultants, temporary and other workers at PCSD must adhere to this procedure. All routers and switches connected to PCSD production networks are affected.

3. Procedure

Every router must meet the following configuration standards:

- Only one local user account is configured on the router, used for backup if an external authentication source is not reachable. Routers and switches must use RADIUS for all user authentications.
- 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.
- Only authorized tech support employees are allowed to login to a router or switch. The Technology Director or Network Engineer can give an employee rights.

The following services or features must be disabled:

- IP directed broadcasts
- Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
- TCP small services
- UDP small services
- All source routing and switching
- All web services running on router
- Cisco discovery protocol on Internet connected interfaces
- Telnet, FTP, and HTTP services
- Auto-configuration

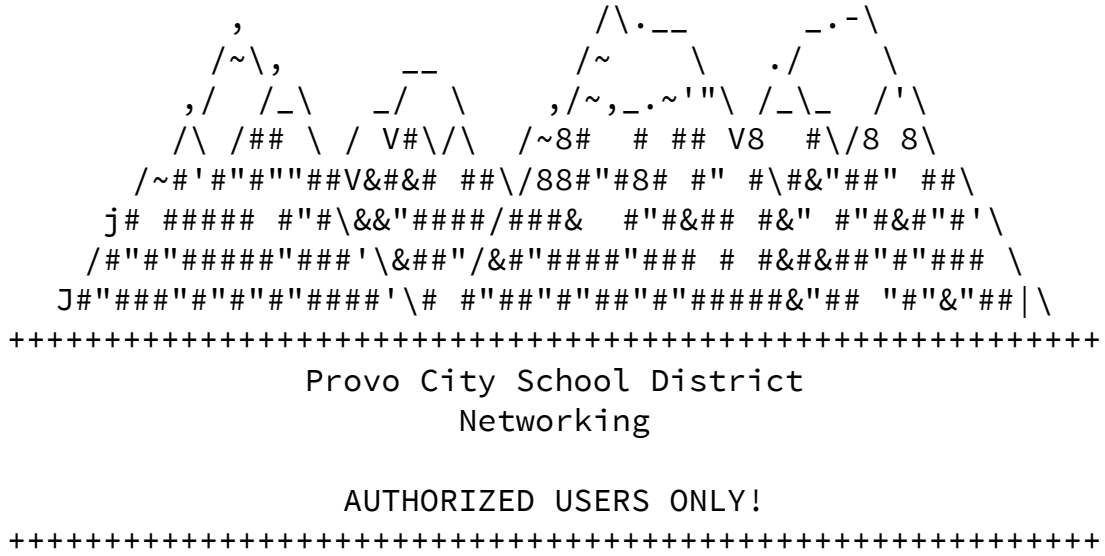
The following services should be disabled unless a business justification is provided:

- Dynamic trunking
- Scripting environments, such as the TCL shell

The following services must be configured:

- Password-encryption

- NTP configured to a corporate standard source
- All routing updates shall be done using secure routing updates.
- 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, at least v2.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- Access control lists for transiting the device are to be added as business needs arise.
- Each router must have the following statement presented for all forms of login whether remote or local:



- 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.
- Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
- 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:
  - IP access list accounting
  - Device logging
  - Incoming packets at the destination router with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
  - Router console and modem access must be restricted by additional security controls