**Router Security Policy**

**1.0 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 ***<Company Name>.***

**2.0 Scope**

All routers and switches connected to ***<Company Name>*** production networks are affected. Routers and switches within internal, secured labs are not affected.

**3.0 Policy**

Every router must meet the following configuration standards:

* No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.
* The enable secret password on the router must be kept in a secure encrypted form.
* The router must have the enable secret password set to the current production router password from the Network Operations organization. The enable password command should not be used.
* Routers that do not meet these standards will be re-engineered as needed.
* Disallow the following:
* Incoming packets at the router sourced with invalid addresses such as RFC1918
* Incoming packets at the router sourced with ***<Company Name>*** addresses (spoofing)
* TCP and UDP “small services”
* All source routing
* All web services running on router
* IP directed broadcasts
* Cisco Discovery Protocol (CDP) on all Third Party interfaces
* Use corporate standardized SNMP community strings. Community strings “public” and “private” should never be used.
* Every router should save system logging information to a local RAM buffer in addition to a secured “syslog” server.
* Any VTY (Virtual Terminal) should be configured to accept connections only with the protocols actually needed. (SSH should be used when possible.) VTY timeouts and a restrictive access-class should be enforced.
* Each router must have the following statement posted in clear view:

**NOTICE:**  This system is to be used ONLY by AUTHORIZED personnel. Any unauthorized use of the system is unlawful, and may be subject to civil and/or criminal penalties. Use of the system may be logged or monitored without further notice.

* All routers must be included in the corporate enterprise management system (MRTG and Network Node Manager) with a designated point of contact.
* Security patches and IOS upgrades will be applied as needed during a designated maintenance window. It is the responsibility of the Network Operations organization to keep up-to-date with new security vulnerabilities.

Every switch must meet the following configuration standards:

* Ports without any need to trunk, should have any trunk settings set to off, as opposed to auto.
* Trunk ports should use a virtual LAN (VLAN) number not used anywhere else in the switch.
* Disable any port that is not needed.
* Disable Spanning Tree Portfast on any port that is attached to a router, firewall or load balancing switch.
* Hard code speed and duplex settings on all ports, as opposed to auto.
* Core switches must be assigned a private internal IP address in a “management VLAN.”

**Source:** <http://www.murchison.net/techno/router-secpol.html>