Router Security Policy

CS Department 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 SUNY Stony Brook CS department.

2.0 Scope
All routers and switches connected to SUNY Stony Brook CS department production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

3.0 Policy
Every router must meet the following configuration standards:

1. No user accounts are configured on the router.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
   a. IP directed broadcast
   b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
   c. TCP small services
   d. UDP small services
   e. All source routing
   f. All web services running on router. If required to maintain the router then it should only be enabled when maintenance is occurring. All access controls should be enabled.
4. Use department standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the department enterprise management system with a designated point of contact.
7. The router should be placed in a location where physical access is limited to authorized persons only
8. Each router must have the following statement posted in clear view:

"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."

Every network switch must meet the following configuration standards:
1. No user accounts are configured on the switch
2. The enable password on the switch must be kept in a secure encrypted form. The switch must have the enable password set to the current production switch password from the switch's support organization.
3. Use department standardized SNMP community strings.
4. The switch must be included in the department enterprise management system with a designated point of contact.
5. The switch should have MAC level address locking enabled if the option is available
6. The switch should generate an SNMP trap if the link drops and is re-established if the feature is available
7. The switch should disable a port or group of ports if new or unregistered MAC addresses appear on a port if the feature is available

8. The switch should be placed in a location where physical access is limited to authorized persons only.
9. The switch should have any web server software disabled and if required to maintain the switch the server should be started to configure the switch and then re-disabled. All access controls to administrative functions should be enabled (host/login-password/network)
10. Each switch must have the following statement posted in clear view:

"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."

4.0 Enforcement
Any users found to have violated this policy may be subject to disciplinary action.

5.0 Definitions

Terms	Definitions
Production Network	The "production network" is the network used in the daily business of SUNY Stony Brook CS department. Any network connected to the department backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to SUNY Stony Brook CS department employees or impact their ability to do work.
Lab Network	A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, research, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to SUNY Stony Brook CS department nor affect the production network.

6.0 Revision History