MSG Router and Switch
Standard Operating Procedure

Document Number:	IRNG-SOP-0006
Business Unit:	Infrastructure Engineering
Process Owner:	Lenny Guardino
Process Owner Email:	Lenny.Guardino@msg.com
Written by:	Adrienne Myers, MS, CISSP
Go Live:	

Foreword: This document prescribes the 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 Madison Square Garden Company (MSG).

Contents

1 Purpose and Goals

1.1 Purpose

Routers and switches physically (and virtually) separate logical networks through configuration and protocol management. Effective management of these important network devices helps to protect internal network resources from external risks. This Standard Operating Procedure (SOP) provides protocol standards to minimize security and intrusion risks related to internal resources from outside influences.

This SOP covers the following IT security controls; DS 1.4, DS 1.5, DS 3.7 - 3.8, DS 9.0. See the IT Security Controls Table file MSGT-REQ-0001 located in the IT Infrastructure Library\MSG Tech folder here.

1.2 Audience

All employees, contractors, consultants, temporary, vendors, contingent and other workers at MSG and its subsidiaries must adhere to this SOP.

1.3 Scope

All routers and switches connected to MSG production networks are affected.

2 Procedure

Every router and switch deployed on MSG's production network must meet the following configuration standards:

1. Routers and switches must use TACACS+ for all user authentication.
2. The enable secret on the router or switch must be kept in a secure encrypted form.
3. The router or switch must have the enable secret set to the current production router/switch password from the device's support organization.
4. 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
5. The following services should be disabled unless a business justification is provided:
    a. Dynamic trunking
    b. Scripting environments, such as the TCL shell
6. The following services must be configured:
    a. Password-encryption
    b. NTP configured to a corporate standard source
    c. All routing neighbors must exchange secure routing updates
    d. 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.
    e. Disable SNMP (Simple Network Management Protocol) if it is not in use or use only SNMPv3 or higher and select SNMP community strings that are strong passwords. (See MSG Password-Passphrase Policy ISEC-POL-0002)
    f. Access control lists must be used to restrict traffic for SNMP Read Only and Read Write purposes.
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. All unused core switch ports must be disabled. Access layer switch ports should be disabled whenever practical, and where the needs of the business permit.

11. Media Access Control (MAC) address filtering must be enabled on active switch ports where practical and needs of the business permitting.
12. Network-based access control must be implemented on all routers and switches.
13. Logging must be enabled on all routers and switches.
14. Where layer 2 switches are deployed, a firewall, router, or other higher layer network communications device must provide network isolation / traffic control.
15. Each router must have the following statement presented for all forms of login whether remote or local see Figure 1:

```
~~ This equipment is for authorized use only.  Unauthorized use of this ~~~

~~ equipment is prohibited by law.  All usage is monitored and logged. ~~~

**************************************************************************
```

Figure 1 - Login Banner

16. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. Secure Shell (SSH) version 2 is the mandatory management protocol.
17. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
18. 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. Explicit deny IP any/any logging
    b. Log counters against successful hits
    c. Device logging
19. 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 on sensitive devices.
20. Router console and access must be restricted by additional security controls.
21. A regular (e.g. monthly) process to identify and evaluate patches for routers and switches must be implemented.
22. Routers and switches must be kept updated to patch levels that address significant security vulnerabilities.
23. Critical patches must be addressed within 48 hours of release.
24. A centrally managed patch management system for the routers and switches should be deployed.

3 Procedure Compliance

3.1 Compliance Measurement

The Information Security team will verify compliance to this SOP through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the SOP owner.

3.2 Exceptions

Any exception to this SOP must be approved by the IT Infrastructure Senior Vice President in advance.

3.3 Non-Compliance

An employee or contingent worker found to have violated this SOP may be subject to disciplinary action.

3 Review and Approval

Name	Title	Signature	Date
Adrienne D Myers	Technical Writer	Adrienne Myers	4/9/2020
Matthew Horowitz	Director		
Lenny Guardino	Vice President		

Contributors			
Victor Leung	Security Architect	Colin Campbell	Sr. Network Engineer
Khiry Marshall	Network Engineer	Adriano Sverko	Technical Writer
Jason Purrone	Network Engineer		

Effective Date: **Review Date:**

Revision History

Version	Writer	Notes	Date
1.0	Adrienne Myers, MS, CISSP		