NATIONAL DATA
MANAGEMENT AUTHORITY

Router and Switch Security Policy

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This policy addresses the secure configuration of routers and switches.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

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 the Government of Guyana.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this policy. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This policy encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It specifically addresses all routers and switches connected to the Government of Guyana's Networks. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organisation's Information Security Policy and its associated standards.

4.0 Information Statement

While switches connect computers within a single network, routers are used to connect entire networks to each other. Given that both types of devices are used to facilitate information sharing, it is crucial that they are optimally configured to mitigate risks of compromise to an organisation's network.

5.0 Policy

5.1 Every router must meet the following configuration standards:

5.1.1 Local admin only user accounts are configured on the router. Routers and switches must use Terminal Access Controller Access Control System+ (TACACS+ or RADIUS, or LDAP) for all other user authentications.

5.1.2 The enable password feature 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.

5.1.3 Enable account lockouts for three (3) unsuccessful login attempts.

5.1.4 Enable user lockout if the terminal prompt is idle for five (5) minutes.

5.1.5 Web services on a router provide a useful method of managing devices. It can be enabled but must be restricted to a subnet that authorised users will connect from.

5.1.6 LLDP/CDP is useful for troubleshooting. These protocols can be enabled on switch-switch links but disabled on interfaces that clients connect from

5.1.6.1 Anti-spoofing techniques For customers with multiple devices DHCP snooping must be enabled to protect from rogue DHCP servers.

5.1.7

5.1.8 The following services or features must be disabled:

5.1.8.1 Internet Protocol (IP) directed broadcasts

5.1.8.2 Transfer Control Protocol (TCP) small services

5.1.8.3 User Datagram Protocol (UDP) small services

5.1.8.4 All source routing.

5.1.8.5 All web services running on router

5.1.8.6 CDP, LLDP discovery protocol on interfaces

5.1.8.7 Telnet, File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP) services

5.1.8.8 Auto-configuration

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

5.1.9.1 Dynamic trunking

5.1.9.2 Scripting environments, such as the TCL shell

5.1.10 The following services must be configured:

5.1.10.1 Password encryption

5.1.10.2 Network Time Protocol (NTP) Configured to a corporate standard source.

5.1.11 All routing updates shall be done using secure routing updates.

5.1.12 Use corporate standardised Simple Network Management Protocol (SNMP v.2c or higher) 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.

5.1.13 Access control lists must be used to limit the source and type of traffic that can terminate on the control panel.

5.1.14 Access control lists for transiting the device are to be added as business needs arise.

5.1.15 The router must be included in the corporate enterprise management system with a designated point of contact.

5.1.16 Each router must have the following statement presented for all forms of login whether remote or local: *"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. Use of this system shall constitute consent to monitoring."*

5.1.17 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.

5.1.18 Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

5.1.19 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:

5.1.19.1 Device logging.

5.1.19.2 The router should filter on the Internet WAN inbound interface all packets sourced from bogon prefixes[1] except RFC1918 addresses that are authorized by the Internet Service Provider for infrastructure support services such as DNS or NTP.

5.1.19.3 Routers must be configured with a stateful firewall to only allow connections to be initiated from the LAN.

5.1.19.4 Router console and modem access must be restricted by additional security controls.

5.1.19.5 All login and logout events must be logged.

6.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the policy may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector

[1] Retrieved from https://bgpfilterguide.nlnog.net/guides/bogon_prefixes/

Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

7.0 Exceptions

Requests for exceptions to this policy shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein.

8.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this policy.

9.0 Definitions of Key Terms

Term	Definition
Remote Access[2]	Access to an organisational information system by a user (or an information system) communicating through an external, non-organisation-controlled network (e.g., the Internet).
Router[3]	A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets.
Switch[4]	A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination.

10.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[2] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/remote_access
[3] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/router
[4] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center CSRC https://csrc.nist.gov/glossary/term/switch