NETWORK DEVICE MANAGEMENT (NDM) SECURITY REQUIREMENTS GUIDE (SRG) OVERVIEW

Version 4, Release 2

27 April 2023

Developed by DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 1
1.4 SRG and STIG Distribution 2
1.5 Document Revisions 2
1.6 Other Considerations 2
1.7 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 NIST SP 800-53 Requirements 4
2.2 General Procedures 4

3. CONCEPTS AND TERMINOLOGY CONVENTIONS 5

3.1 Network Device Management (NDM) Scope 5

4. GENERAL SECURITY REQUIREMENTS 7

4.1 Management Network 7
4.2 Network Device Access 7
4.3 Out-of-Band Management Network 7
4.4 In-Band Management Network 8
4.5 Simple Network Management Protocol (SNMP) 8
4.6 Logging 8
4.7 Syslog Server 9
4.8 Account Management and Access Control 9
4.9 Communications Servers 9
4.10 Authentication, Authorization, and Accounting (AAA) Servers 9
4.11 Local Accounts 10
4.12 Communications Encryption 10
4.13 Network Management Auxiliary Components 10
4.14 NTP Servers 11
4.15 SNMP Manager 11
4.16 Image and Configuration Storage 11

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

This Network Device Management (NDM) Security Requirements Guide (SRG) provides the technical security policies and requirements for applying security concepts to systems. This document details NDM security practices and procedures applicable to the management of all DOD network devices (e.g., routers, firewalls, application layer gateways, intrusion detection/ prevention systems), except where a product specific STIG exists. This SRG does not address the configuration of NDM clients (e.g., the workstations used to manage network devices). Each of these clients' security postures should be validated with the STIG for the underlying technology or operating system. It is assumed that if the NDM is installed on a base platform (e.g., an operating system); the base platform is STIG-compliant.

1.2 Authority

DOD Instruction (DODI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 SRG and STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DOD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DOD Risk Management Framework (RMF). DOD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 NIST SP 800-53 Requirements

All applicable baseline technical NIST SP 800-53 requirements and security best practice requirements are included in this SRG.

CNSSI 1253 defines the required controls for DOD systems, based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

2.2 General Procedures

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured system. These procedures are not product specific and are intended for use when a product-specific STIG is not available.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

This section provides background information on NDM technology. This overview is not intended to be used as a comprehensive source of information on NDM technology or DOD network architectures. The focus is placed on providing a background for security considerations and supplementary information to help understand terminology used in the SRG requirements and procedures.

3.1 Network Device Management (NDM) Scope

As the name implies, network device management (NDM) is the management aspect of network devices, such as routers, firewalls, application layer gateways (ALG), and intrusion detection/prevention systems (IDPS). NDM is built into these devices, functioning in a way similar to an operating system. In fact, NDMs are often composed of a set of tools that exists as part of the device's operating system, while in other cases an NDM is a specialized application sitting on top of an operating system. While an NDM is not synonymous with a general operating system, it performs many of the same functions, including the following:

- Management interface protection.
- Administrator account management.
- Management session security.
- Management protocols.
  - Administrator use (e.g., SSH, HTTPS).
  - Machine to machine (e.g., SNMP, NTP, syslog).
  - Auditing.
- Device code upgrades/patches.
- Device configuration protection.
- Performance monitoring.

Requirements are included in the NDM SRG when they are applicable to network devices in general and not just to one or two specific network device types. The NDM requirements apply to all network devices regardless of network function. Specific network technology SRGs will provide requirements for the network function of the device. For example, the requirements in the Router SRG focus on routing protocols, packet forwarding, and related matters but do not address user account requirements, as these are covered by the NDM SRG. If you were implementing a router, you would use both the Router SRG and the NDM SRG together to gather your requirements. The intention of having the NDM SRG separate from the network technology SRGs is to streamline the SRG process for the network devices that provide multiple network functions because they share a common configuration and management platform.

Network devices generally operate on three planes (areas of operations): the Management Plane, the Control Plane, and the Data Plane.

- The Management Plane handles administration of the network device itself. This subject is addressed in the NDM SRG.

- The Control Plane handles the routing and signaling functions. This is the focus of the Router SRG.

The Data Plane handles traffic inspection and flow functions. This is addressed in the Firewall SRG, ALG SRG, IDPS SRG, etc.

4. GENERAL SECURITY REQUIREMENTS

NDM technologies enable the management of network devices such as routers, firewalls, Application Layer Gateways, and Intrusion Detection and Prevention Systems. Most of the material in this section has been derived from the DISA document "Network Management—Network Operations Center Security Guidance At-a-Glance." Readers can refer to that publication for more detailed information on the basics of NDM security. This section provides a condensed version of the material covered in that publication as well as relevant information it does not cover.

4.1 Management Network

Management systems provide the network operator the facility to manage the network and all of its components. They are both the platforms and applications that interact with the managed network devices to provide the administrators a framework to facilitate Operation, Administration, Maintenance, and Provisioning (OAM&P) tasks. OAM&P is a group of management functions that enable system or network fault indication and diagnostics, performance monitoring, security management, configuration management, and service provisioning. Management systems and managed network devices need to be interconnected. The facility that provides this connection is referred to as the management network.

To be managed, a network device utilizes a management interface to communicate with management systems. The management network is composed of network management workstations, authentication servers, syslog servers, communications servers, Operations Support System (OSS), and a network for transporting management traffic.

4.2 Network Device Access

To provide management access, network devices support direct serial connections, out-of-band connections, and in-band connections. Either in-band or out-of-band connections are used to transport network management messages between the managed network devices and the management systems used for providing OAM&P functions. In either case, the same services such as telnet, SSH, HTTP, and SSL are used to access a managed network device.

The direct serial interface is typically referred to as the craft port or console port. There may also be an auxiliary port. This interface is intended to be an access port through which code downloads and local monitoring and control can take place. The auxiliary port, console port, and any slow-speed async serial port with an analog modem connected to it provide the capability for direct dial-up administrative access.

4.3 Out-of-Band Management Network

The Out-of-Band Management (OOBM) network is an IP network used exclusively for the transport of OAM&P data from the network being managed to the OSS components. Its design provides connectivity to each managed network device, enabling network management traffic to flow between the managed network devices and the management workstations. This allows the

use of paths separate from those used by the network being managed. The management workstations can be located locally or remotely at a single site or multiple sites, all connecting to the OOBM network. OOBM networks isolate users' traffic from network management traffic.

The management interface can be a true OOBM interface or a standard interface functioning as the dedicated interface. In either case, the management interface of the network device will be directly connected to the OOBM network.

An OOBM interface does not forward transit traffic, thereby providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device. If the device does not have an OOBM port, the interface functioning as the management interface must be configured so that management traffic does not leak into the managed network and production traffic does not leak into the management network.

4.4 In-Band Management Network

The in-band management paradigm exists when the management traffic takes the same data path as nonmanagement or production traffic, thereby using the same physical or logical interface. Management plane traffic shares the same path as the control plane and forwarding plane. Therefore, network management traffic is intermixed with user traffic using the same interfaces of the network devices being managed.

Applications used to access the managed device utilize TCP as the transport protocol. The TCP keepalive feature will periodically verify that the remote node of the management session (i.e., the network management station) is still reachable. In the event the remote node has abnormally terminated or an upstream link from the managed device is down, the management session will be terminated, thereby freeing device resources and eliminating any possibility of an unauthorized user being orphaned to an open idle session of the managed device.

4.5 Simple Network Management Protocol (SNMP)

SNMP version 3 (SNMPv3) provides secure exchanges of management data between network devices and network management systems by providing authentication, privacy, and access control functionality. The encryption and authentication features in SNMPv3 ensure high security in transporting packets to a management console. SNMPv3 employs the User-based Security Model (USM) to provide cryptographic services. Data can be collected securely from correctly configured SNMP devices without fear of the data being compromised. SNMP Set command packets that change a router's configuration can be encrypted to prevent their contents from being exposed on the network.

4.6 Logging

Logging is a key component of any security architecture and is a critical part of network device security. Logging is also essential in assisting with the maintenance and repair of the network. It

lets essential security personnel know what is being done, what was attempted, and by whom it was attempted in order to compile an accurate risk assessment. It is also imperative that all configuration changes to network devices are logged on a per-session and per-user basis. Maintaining an audit trail of system activity logs can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network.

4.7 Syslog Server

A syslog server provides the network administrator the ability to configure all of the communication devices on a network by sending log messages to a centralized host for review, correlation, reporting, and storage. This implementation provides easier management of network events for monitoring and automatic generation of alert notification. The repository of messages facilitates troubleshooting when problems are encountered and can assist in performing root cause analysis that allows an administrator or analyst to view the "big picture" of the network operations. Syslog files can be parsed in real time to identify suspicious behavior or archived for review at a later time for research and analysis.

4.8 Account Management and Access Control

Information security vulnerabilities are inherent in all forms of computer systems, software, architectures, and devices. The goal of information security is to provide data integrity, confidentiality, and availability. In order to provide these services to the DOD community, general security standards for any form of remote access to a DOD network must be in place. These standards are set forth for ease of configuration management and to aid in developing a secure, standardized remote access environment. Restricting access to all network devices is critical in safeguarding the network.

4.9 Communications Servers

A communications server (terminal server) can be used to provide interconnectivity between all managed network devices and the OOBM gateway router for administrative access to the device's console port. In the event the OOBM network is not able to provide connectivity due to an outage, the communications server can provide a dial-up PPP connection to access a network device. The auxiliary port, console port, and any slow-speed async serial port with an analog modem connected to the managed device also provide the capability for direct dial-up administrative access to infrastructures that do not have a communications server for management access.

4.10 Authentication, Authorization, and Accounting (AAA) Servers

An Authentication, Authorization, and Accounting (AAA) server manages user requests for access to network resources. Authorization is the method used to describe what resources users have access to once they have been authenticated. Authorization is the method used to describe what users have the right to do once they have been authenticated. Accounting or auditing is the

component that keeps track of the services and resources accessed by the users. This information can be used later for resource tracking or troubleshooting.

AAA servers provide services by interacting with and managing account databases and directories containing user information with network access points and gateway servers. AAA services allow for the enforcement of policy, audit of user activity, and access to network resources. Some of the methods by which devices or applications communicate with an AAA server are the Remote Authentication Dial-In User Service (RADIUS) specification or Terminal Access Controller Access Control System (TACACS+) protocol.

Using standardized authentication protocols such as RADIUS, TACACS+, and Kerberos provides centralized authentication, authorization, and auditing services for management of network components. Authentication servers are very scalable as they support many user accounts and authentication sessions with the network components. They allow for the construction of template profiles or groups given authorization for specific tasks and access to specific resources. Users are then given an account that has been configured in the authentication server and has been assigned to a group.

4.11 Local Accounts

An NDM technology is assumed to support only administrator-level accounts, not user-level accounts. User-level accounts may be supported by a technology in the Data Plane, such as an ALG, that has the concept of standard users, but most network technologies are directly used and/or administered by administrators only. Therefore, NDM requirements involving accounts are based on the assumption that they are only applicable to administrator-level accounts.

Of special importance is the emergency administration account, which is sometimes referred to as the account of last resort or as the emergency troubleshooting account. This account is used only when the authentication server is off line or not reachable via the network. Requirements concerning account inactivity or the maximum password lifetime do not apply to this account. Note that currently only one emergency administration account on each device is allowed.

4.12 Communications Encryption

An NDM technology is assumed not to be responsible for encrypting communications passing through it. Encryption is the responsibility of the endpoints of the communication session or a host acting on behalf of an endpoint, such as a VPN server. Also, by definition, encrypting communications involves architectural considerations because both endpoints, and the devices acting on behalf of the endpoints, must work together to establish and maintain the encryption for the communications.

4.13 Network Management Auxiliary Components

The network management auxiliary components are used to provide capabilities to enable both management and security functionality for the managed network. These components are being secured as a result of the IA requirements that have been defined based on the topology, that is,

whether they are residing within a dedicated OOB network infrastructure or are connected to an in-band network. Nevertheless, since they do have sessions with elements in the managed network that could be compromised, there are additional IA measures that must be followed to reduce the risk of these components also being compromised.

4.14 NTP Servers

NTP provides an efficient and scalable method for managed network devices to actively synchronize to an accurate time source. Ensuring NTP servers are always available to provide time is critical, and it is imperative all single points of failure for the NTP infrastructure are eliminated. Knowing the correct time is crucial not only for proper network functioning but also for security. Compromising an NTP server opens the door to more sophisticated attacks that include NTP poisoning, replay attacks, obfuscation/alteration of logging data, and denial of service. To provide security through separation and isolation, the NTP server should only be connected to the management network. This enables the NTP server to provide time using a secure path to managed devices. If the NTP server is not an appliance, it is critical that the system is secured by maintaining compliance with the appropriate OS SRG or STIG.

If NTP is not authenticated, an attacker can introduce a rogue NTP server. This rogue server can then be used to send incorrect time information to network devices, which will make log timestamps inaccurate and affected scheduled actions. NTP authentication is used to prevent this tampering by authenticating the time source.

4.15 SNMP Manager

The SNMP manager provides the interface between the network management personnel and the managed network. The SNMP agent provides the interface between the manager and the device being managed. The manager is the collector of alarm information via SNMP traps as well as statistical and historical management information retrieved by polling the agents within the managed network. This information is vital for real-time monitoring, alarm management, strategic planning, and performance management. IA measures must be implemented to mitigate the risk of the SNMP manager being compromised. To provide security through separation and isolation, the SNMP manager must only be connected to the management network. This enables the SNMP manager to provide management services to the managed devices using a preferred secure path. Many SNMP managerial functions have been rolled into a network administration application or Security Information and Event Management (SIEM) tool.

4.16 Image and Configuration Storage

It is important to keep the device configurations and the device system files synchronized in case there is a power failure or other problem that forces the device to restart. File synchronization will ensure managed devices will load the correct configurations and system files. If there is a need to revert to an older configuration, it should be stored off-line.

Images installed on the devices can become corrupt. Hence, it is imperative to retain a copy of the current production images on some form of off-line media or file server. Both prior and new

image versions must also be kept in case an event regression occurs or for planned upgrade migrations, respectively.

With the image and configuration files stored off-line, the files must be transferred to and from the device using a secure method. Both FTP and TFTP are unencrypted, so it is required that a secure method be used instead. The following are some alternative approaches:

- Copies of the device configuration can be archived on the device's flash or hard drive if the media is available.
- Copy and paste output of a displayed configuration while in an SSH session or console connection. The file can then be saved onto an external media source and stored in a secure location.
- Whenever possible, the preferred method is to use Secure Copy Protocol (SCP), which requires that AAA be configured in order for the device to determine whether the user has the correct privilege level.