RIVERBED NETIM SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

11 September 2025

Developed by Riverbed and DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Riverbed NetIM Security Technical Implementation Guide (STIG) provides security policy and technical configuration requirements for the use of the Riverbed SteelCentral NetIM appliances in the Department of Defense (DOD).

Riverbed NetIM is a network monitoring and troubleshooting tool that provides visibility into IT infrastructure by mapping network topology, detecting performance issues, tracking configuration changes, mapping application network paths, and allowing users to diagnose network problems through detailed diagrams.

Key functions of Riverbed NetIM:

- Network discovery and mapping: Automatically discovers network devices and their connections to create a visual representation of the network topology.
- Performance monitoring: Tracks key network metrics like bandwidth utilization, packet loss, latency, and CPU usage to identify performance bottlenecks.
- Application path mapping: Identifies the network path traversed by specific applications to pinpoint performance issues related to application delivery.
- Configuration management: Tracks changes in device configurations and alerts users to potential issues arising from configuration modifications.
- Troubleshooting tools: Provides features like packet capture and analysis to diagnose network connectivity issues.
- Alerting and reporting: Generates alerts based on predefined thresholds and provides detailed reports on network performance and health.

To provide these functions, NetIM can login to network devices. Thus, securing the operating system, management interfaces, and network communications is imperative.

The Riverbed NetIM STIG covers both the Ubuntu operating system and the NetIM application management functions. Requirements for configuring the reporting, traffic analysis, or workflow configuration functions is out of scope but must be specified in the site's System Security Plan (SSP) and configuration documentation.

1.2 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

Category	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.

1.3 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD 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/.

1.4 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.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 AO. 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 DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.7 Product Approval Disclaimer

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). Department of Defense 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 in accordance with (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) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Process

A security assessment of Riverbed NetIM must consist of a security review of both the management backplane and the operating system (OS) security functions. The following STIGs are required as part of all assessments.

2.1.1 Riverbed NetIM OS STIG

The Riverbed NetIM OS STIG contains requirements applicable to review and secure the OS, which is installed by the vendor on the appliance. Many requirements are set by the vendor as part of the VM. NetIM software upgrades include updates for Ubuntu, including any version changes. At the time of initial configuration, sites must use this STIG to secure the OS, enable AAA, and NTP services. This requires access to sudo commands and a challenge/response process with the vendor. Beyond initial configuration, system administrators should limit use of the NetIM shell access, but most critically, limit access to the Bash shell.

Accessing bash commands requires the sysadmin to type "Challenge" at the NetIM shell, then use the site's support email account to send the Challenge code and receive the Response code. DISA requires system admins to immediately log out of NetIMAdmin once the required bash access is no longer needed to mitigate the risk of this superadmin access being inadvertently used. This process may be needed as part of the security review while reviewing the Riverbed NetIM OS STIG for compliance.

Admins must not leave the Bash shell open for long periods without logging out.

An Ubuntu Pro license is required to comply with the FIPS 140-2/140-3 validation requirement.

2.1.2 Riverbed NetIM NDM STIG

The Riverbed NetIM NDM STIG contains requirements applicable to securing the NetIM management plane.

The minimum NetIM software version is 2.10 or later to meet all DISA security requirements. This ensures the capture of required audit records and other security updates.