JUNIPER SRX SERVICES GATEWAY (SG) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

23 April 2021

Developed by 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 DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Juniper SRX is a series of hardware platforms that consists of two product lines, the branch series and the data center series. The two product lines differ based on support for the number and types of available interfaces, traffic throughput capacity, and the network services provided. All platforms share a common design architecture consisting of a Routing Engine (RE) and a Packet Forwarding Engine (PFE). The Junos 12.1X46 is the minimum required version for DoD. The Juniper SRX Services Gateway (SG) STIG is a package of the following:

- Juniper SRX SG Application Layer Gateway (ALG) STIG
- Juniper SRX Services Gateway (SG) Intrusion Detection and Prevention System (IDPS) STIG
- Juniper SRX SG Network Device Management (NDM) STIG
- Juniper SRX SG Virtual Private Network (VPN) STIG

The Juniper SRX Services Gateway SG ALG STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the Juniper Networks SRX multifunction platforms to secure network firewall services. Firewall services, including security policies, zones, and packet inspection, are integrated into the other roles provided by the Juniper SRX. The Juniper SRX SG ALG STIG is used to secure the firewall services implemented by the PFE. The scope of the Juniper SRX SG ALG STIG includes only the default firewall services, such as security policies, zoning, and stateful/stateless content filtering. The Juniper Networks ALG license is a separate product and is not within the scope of this STIG. The Juniper SRX SG NDM STIG and the Juniper SRX ALG STIG are also required to secure the device when used as a firewall in the network architecture.

The Juniper SRX SG NDM STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the Juniper Networks SRX multifunction.

The Juniper SRX SG VPN STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the Juniper Networks SRX multifunction platforms when configured for network IPsec VPN role in the architecture. A license for two VPN connections is available by default; however, an additional license is required if more VPN connections are needed. The Juniper SRX SG VPN STIG is used to secure the VPN services implemented by the PFE. The scope of the Juniper SRX SG VPN STIG includes site-to-site, which connects two VPN gateways and remote access (dynamic) VPNs. The Juniper SRX SG NDM STIG and the Juniper SRX SG ALG STIG are also required to secure the device.

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   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   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 For Official Use Only (FOUO) will be available for those 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.

1.6 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.

1.7 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.

1.8 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 Security Assessment Information

A security assessment of the Juniper SRX firewall must consist of a security review of both the RE and the PFE services functions. The minimum required documents are the Juniper SRX NDM and the Juniper SRX ALG STIGs.

Additionally, because the Juniper SRX SG can also be configured as a router, switch, and various other capabilities, a complete security assessment requires assessing all roles and functions used in the specific DoD implementation. Since product STIGs are not available for all roles, use of existing generic technology STIGs may be required to secure these functions. For example, router and Layer 3 switching requirements are addressed in the Network Perimeter Router L3 Switch STIG