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

Version 1, Release 1

28 March 2016

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

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Juniper SRX SG STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the SRX series multifunction platforms by Juniper Networks. The STIG is a package of four STIGs that together ensure the secure implementation of the Network Device Management (NDM) function and the firewall, Intrusion Detection and Prevention System (IDPS), and Virtual Private Network (VPN) traffic services.

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 Juniper SRX SG STIG consists of four documents. The Juniper SRX SG NDM STIG is used to secure the RE functions, such as the Junos software, management functions, device protection, and internal information flow control. The Junos 12.1X46 is the minimum required version for DoD. The Juniper SRX SG Application Layer Gateway (ALG) STIG is used to secure the firewall configuration, which is integrated into all roles of the PFE. The Juniper SRX SG IDPS STIG is used to secure the IDPS configuration when implemented by the PFE. The Juniper SRX SG VPN STIG is used to secure the IPsec VPN configuration when implemented by the PFE.

Additionally, because the Juniper SRX SG can also be configured as a router, switch, and various other roles in the network architecture, a complete security assessment requires assessing all roles used in the specific DoD implementation. Each security review must include the Juniper SRX SG NDM STIG and Juniper SRX SG ALG STIG, at a minimum, regardless of the role in the network architecture or licenses installed. 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.

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 Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.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

2.1 Security Assessment Information

A security assessment of the Juniper SRX must consist of a security review of both the RE and the PFE services functions. Thus, the Juniper SRX SG NDM STIG and the Juniper SG ALG STIG are required for all security reviews, regardless of the network roles configured on the device. Additionally, all roles (e.g., VPN, IDPS) configured must be subjected to a security assessment using the applicable STIG.

Because of the complexity and flexibility of Junos and the SRX series architecture, the stanzas given in the checks and fixes are examples only. There are often several different methods for meeting a requirement. Additionally, there are some feature differences between the branch and higher-end devices that have been taken into consideration whenever that information was available in the limited testing environment or knowledge base. Reviewers will need to work with the site representative to determine if alternate stanzas meet the intention of the requirement.