

UNCLASSIFIED



# **ROUTER SECURITY REQUIREMENTS GUIDE (SRG) TECHNOLOGY OVERVIEW**

**Version 4, Release 3**

**24 April 2024**

**Developed by DISA for the DOD**

UNCLASSIFIED

### 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

	<b>Page</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Executive Summary.....	1
1.1.1 Security Requirements Guides (SRGs) .....	1
1.1.2 SRG Naming Standards .....	2
1.2 Authority.....	2
1.2.1 Relationship to STIGs.....	2
1.3 Vulnerability Severity Category Code Definitions .....	3
1.4 SRG and STIG Distribution.....	3
1.5 Document Revisions .....	3
1.6 Other Considerations.....	3
1.7 Product Approval Disclaimer .....	4
<b>2. ASSESSMENT CONSIDERATIONS.....</b>	<b>5</b>
2.1 NIST SP 800-53 Requirements .....	5
2.2 General Procedures .....	5
<b>3. CONCEPTS AND TERMINOLOGY CONVENTIONS .....</b>	<b>6</b>
3.1 Perimeter Router.....	6
3.2 Provider Edge (PE) Router.....	6
3.3 Provider (P) Router .....	6
3.4 BGP Router.....	6
3.5 MPLS Router.....	6
3.6 Multicast Router.....	7
3.6.1 Rendezvous Point (RP) Router.....	7
3.6.2 Designated Router (DR) .....	7
3.6.3 MSDP Router .....	7
3.7 Out-of-Band Management (OOBM) Gateway Router.....	7

## LIST OF TABLES

	<b>Page</b>
Table 1-1: Vulnerability Severity Category Code Definitions .....	3

## 1. INTRODUCTION

### 1.1 Executive Summary

This Router Security Requirements Guide (SRG) provides the requirements for applying security concepts to routers that have been deployed to provide network connectivity, network security, and network services. The scope of this guide will address requirements for routers deployed in enterprise networks (e.g., enclave, data center, JIE-ICAN, etc.) as well as backbone networks (e.g., DISN Core, JIE-WAN, etc.) where each router may assume multiple roles and is responsible for provisioning various network services.

#### 1.1.1 Security Requirements Guides (SRGs)

Security Requirements Guides are collections of requirements applicable to a given technology family. They represent an intermediate step between Control Correlation Identifiers (CCIs) and Security Technical Implementation Guides (STIGs). CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in a policy, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product's technology area.

There are four core SRGs: Application, Network, Operating System, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, Technology SRGs are developed to address the technologies at a more granular level.

This [Technology] SRG is based on the [Parent SRG]. The [Technology] SRG contains general check and fix information that can be used for products for which STIGs do not exist.

The STIGs based on this SRG will provide the product-specific technical implementation guidance for that product. The STIG will contain the specific check and fix information for the product it covers.

#### SRG Hierarchy example:

```
Application SRG
|___Database SRG
    |___Microsoft SQL Server 2016 STIG
```

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and to provide appropriate justification. It also provides the structure to identify variations in specific values based on the technology family. These variations will be captured once and will propagate down to the Technology SRGs and then to the STIGs. This will eliminate the need for each product-specific STIG to address items that are not applicable.

### 1.1.2 SRG Naming Standards

To establish consistency across the SRGs, a naming standard for the Group Title and STIGIDs has been established.

#### Technology SRG Naming Standards

For Technology SRG Group Title and STIGIDs, the following applies:

*{Core SRG value}-{Technology SRG}-{5- or 6-digit numeric sequence number}*

Examples:

*SRG-NET-000001-RTR-000001*  
*SRG-APP-000001-COL-000001*  
*SRG-NET-000001-VVSM-00001*  
*SRG-OS-000001-UNIX-000001*

Checks/fixes will be included at this level in a general form. These checks and fixes will apply for any STIGs that are created for products that do not have product-specific check and fix guidance.

## 1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that 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 [National Security Agency/Central Security Service], 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 must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

### 1.2.1 Relationship to STIGs

The SRG defines the requirements for various technology families, and the STIGs are the technical implementation guidelines for specific products. A single SRG/STIG is not all-inclusive for a given system, which may include but is not limited to Database, Web Server, and Domain Name System (DNS) SRGs/STIGs. For a given system, compliance with all (multiple) SRGs/STIGs applicable to a system is required.

### 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**

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

### 1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: [disa.stig\\_spt@mail.mil](mailto: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

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). 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](mailto: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.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://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 SRG will identify the router role in each requirement. Hence, only requirements that map to the router role or function would be applicable. Requirements that simply state “the router” would be applicable to all routers regardless of whether it has been deployed in an enterprise (e.g., enclave, data center, JIE-ICAN, base, camp, etc.) or backbone network (e.g., DISN Core, JIE-WAN, etc.).

#### 3.1 Perimeter Router

The perimeter router resides at the edge of an enterprise network, providing connectivity to the NIPRNet or SIPRNet. It is responsible for filtering both inbound and outbound traffic that will promote a defense-in-depth security posture in conjunction with other IA components at the edge, such as the firewall and intrusion detection system.

#### 3.2 Provider Edge (PE) Router

The PE router resides at the edge of a backbone network, providing customer connectivity as well as transport services (i.e., MPLS L2VPN and L3VPN) for those customers. It is the interface between the customer edge (CE) router and the IP/MPLS core. With the exception of traffic destined to itself or the core, the PE router does not filter packets.

#### 3.3 Provider (P) Router

The P router resides within the IP/MPLS core of the backbone network. It provides connectivity between the PE routers and the forwarding of transient traffic as unicast, multicast, and MPLS labeled packets.

#### 3.4 BGP Router

A BGP router can reside at the edge of both enterprise and backbone networks, with the exception of route reflectors that will typically reside inside the network. The BGP router will peer with other autonomous systems (eBGP peering) to learn routes from them as well as peer with routers within the local autonomous system (iBGP peering) to share the learned external routes.

#### 3.5 MPLS Router

MPLS provides traffic engineering capabilities to forward traffic independent of the path determined by routing protocols. It is also an enabler for services such as L2VPN and L3VPN that provide connection alternatives to the traditional carrier services. These technologies are dependent on the fundamental MPLS framework, the MPLS tunnel also known as label switch path (LSP). MPLS routers are categorized as either a Label Swap Router (LSR) or edge LSR, also known as a Label Edge Router (LER). The latter is the entry and exit of the MPLS core; that is, they push an MPLS label onto an incoming packet and pop the label off an outgoing packet.

### 3.6 Multicast Router

Multicast routers can reside in both enterprise and backbone networks. They are enabled with Protocol Independent Multicast (PIM) to forward multicast packets toward hosts within the multicast domain that have joined specific multicast groups. Inter-domain multicast provides the capability to discover multicast sources for specific multicast groups from other multicast domains (i.e., autonomous systems) and hence enable hosts to join multicast groups outside of their multicast domain.

#### 3.6.1 Rendezvous Point (RP) Router

RP routers will exist within a Protocol Independent Multicast-Sparse Mode (PIM-SM) multicast domain. PIM-SM supports both shared and source distribution trees that provide the forwarding from the sources to the receivers. For shared trees, PIM-SM establishes the RP as the root of the shared tree. It will receive both PIM Joins and PIM Register messages from Designated Routers.

#### 3.6.2 Designated Router (DR)

DRs can reside in an enterprise network that is enabled for PIM-SM. It is responsible for sending PIM Join, Register, and Prune messages to the RP.

#### 3.6.3 MSDP Router

An MSDP router is a mechanism that connects multicast domains by enabling RPs to share information about active sources within their domains to RPs in other domains. When RPs in remote domains know about the active sources, they can pass on that information to their local receivers, which can then join the multicast group/source. This essentially enables multicast packets to be forwarded between the multicast domains.

### 3.7 Out-of-Band Management (OOBM) Gateway Router

The OOBM gateway router can reside within an enterprise network to provide connectivity between the network elements being managed and the OOBM network. Using dedicated or virtual paths, the OOBM network connects the OOBM gateway routers located at the premise of the managed networks and at the NOC. If the OOBM gateway router is not a device dedicated for the OOBM network (i.e., may be the managed network's premise router), several safeguards must be implemented for traffic containment and separation. Management traffic must not leak into the managed network, and traffic from the managed network must not leak into the management network. Since the managed network and the management network are separate routing domains, separate IGP routing instances must be configured on the router, one for the managed network and one for the OOBM network.