ROUTER
SECURITY REQUIREMENTS GUIDE (SRG)
TECHNOLOGY OVERVIEW

Version 2, Release 2

23 October 2015

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

1. INTRODUCTION

1.1 Executive Summary

This Router Security Requirements Guide (SRG) provides the technical security policies and requirements for applying security concepts to systems. The security requirements contained within the SRGs are applicable to all DoD-administered systems and all systems connected to DoD networks. The SRGs provide requirements to reduce the security vulnerabilities of systems.

This Security Requirements Guide addresses hardening the device and securing the routing functionality only. This includes security of the routing protocols used and the routing table, protection of the device interfaces and resources, and security of services run by the device.
If other functions are implemented by the router device, the security requirements for that functionality must also be applied using additional SRGs and/or STIGs.

SRG requirements must be considered, depending on the specific implementation of the router and the location of the installation (i.e., backbone, enterprise data center, or local network). Device management requirements that relate to management of a device and management access to the device are found in the Network Device Management (NDM) SRG.

1.1.1 Security Requirements Guides (SRGs)

SRGs are collections of requirements applicable to a given technology family. SRGs 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, there are Technology SRGs developed to address the technologies at a more granular level.

This Router SRG is based on the Network SRG. This Router SRG contains general check and fix information that can be utilized 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
        |__MS SQL Server 2005 STIG
```

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and 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

In an effort 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

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 provide 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.

1.2.1 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

	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 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 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 configurations 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% 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.

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 router technology and discusses general security considerations involved with using this technology. This overview is not intended to be used as a comprehensive source of information on router 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 Route Tables

There are two approaches that can be used to safeguard the integrity of a route table: static routes and neighbor router authentication. For obvious reasons, defining static routes is the most secure method and is ideal for small stable networks. When using routing protocols to make route table updates due to changes in network topology and connection states, neighbor router authentication must be used to prevent fraudulent route updates from being received. Authentication occurs when routing updates are exchanged between neighbor routers, thereby ensuring the router receives its routing information from a trusted source.

4. GENERAL SECURITY REQUIREMENTS

Routers perform a critical function; determining optimal paths for traffic and forwarding packets between subnetworks are fundamental to the operation of a network. Aside from the routing function, routers are a control point for the flow of traffic in a network or between networks. This is usually implemented in the form of Access Control Lists, which are simple packet filters; in effect, these are a type of firewall. However, other means of policy enforcement are possible in routers, such as Unicast Reverse Path Forwarding.

4.1 Heading Title

Rather than being a "catchall" for the security requirements of a particular device, the approach of the Security Requirements Guides (SRG) is specific to the function addressed by the particular SRG. This is reflected in this Overview, which only discusses the security issues specific to the routing function.

Routers, as well as other network elements, 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 element itself. This subject is addressed in the Network Device Management SRG.
- The control plane handles the routing and signaling functions. This is the focus of the Router SRG.
- The data plane handles traffic flow functions. Controlling data flow is the function of an Access Control List, which is a packet filtering function.

4.1.1 Routing Protocol Security

Since packet forwarding and path determination are critical, it is imperative that the routing tables be protected. A corrupted or otherwise compromised routing table can lead to wide-scale denials of service or to the loss of confidentiality of information. The routing table can be compromised by the unintentional error of an administrator, by a direct attack by a hostile actor, or by inaccurate routing updates propagated to it by another router. In the last case, it is possible that a router can be adversely affected by an action taken not only outside the organization, but one taken by someone not directly connected to the router. In a route injection attack, an attacker can use a compromised router or forge routing protocol updates to manipulate the routing table of a target router. This can result in the router forwarding traffic to unauthorized destinations where it can be analyzed by the attacker; this can also seriously degrade service for authorized users. Routing updates can be propagated throughout a network in seconds and globally between interconnected networks nearly as rapidly. If this takes place on large, interconnected networks such as the Internet, this can have consequences on a global scale.

Authenticating neighbor router updates effectively counters that threat; routing updates are accepted only if the neighbor router successfully authenticates at each update. The router sending the update sends either a message key or a hash of the key. The receiving router checks the received value against its record; if the values match, the update is accepted. If they do not, the update is rejected.

Although the plain text key or password can be sent, this is not secure since it can be intercepted and is therefore prohibited. Some platforms allow the use of key chains to reduce the risk of a key being compromised. Keys are "chained" together so they are used in sequence; each key has a specified life in which it is active, so it is important that the lifetimes be configured so at least one key is active at any given time and both the sending and receiving routers have their clocks synchronized to the same source. If there is a key mismatch or there is no active key, routing updates cannot take place.

4.1.2 Control Plane Security

Aside from compromising the routing tables, an attacker can impair a router by overwhelming the control plane; this is a form of denial of service (DoS) attack. If it is successful, the normal routing functions may cease to operate, which, in turn, degrades packet forwarding. Therefore, countermeasures must be taken to defend against this:

- The IP address of the router itself should be on its own subnet and that subnet filtered by an ACL.
- Legitimate control plane traffic is identified, and only that traffic is allowed to the router itself by an ACL. Other ACLs control traffic through the router.
- Legitimate control plane traffic is rate limited.
- An ACL is configured to protect against DoS attacks directed against the control plane, such as TCP-SYN attacks.

This approach works in concert with other measures (such as ingress and egress filters) to protect the router. Although vendors refer to these techniques differently, the objective is the same.