INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) SECURITY REQUIREMENTS GUIDE (SRG) TECHNOLOGY OVERVIEW

Version 2, Release 2

24 July 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

Page

1. INTRODUCTION

1.1 Executive Summary

This Intrusion Detection and Prevention System (IDPS) Security Requirements Guide (SRG), along with the Network Device Management (NDM) SRG and associated policy requirements, provides the technical security policies and requirements for network devices that perform traffic inspections up to and including layer 7 of the Open Systems Interconnect (OSI) reference model. This SRG is applicable to the network-based IDPS (including Wireless IDPS) which serve the core functions of an IDS or IPS, regardless of the layer of OSI model used to perform these functions. Host-based IDPSs (HIDS) are not included within the scope of this SRG. This SRG is applicable to the distributed IDPS implementation as a whole, which may include multiple or separate sensors, management consoles, analysis tools, and database used to scan and monitor network traffic.

The core functions of the IDPS are to monitor and analyze incoming and outgoing (e.g., data exfiltration) data traffic and/or system components, alert authorized personnel if hostile or suspicious activity is detected, and take action to block unauthorized activity. The IDPS uses signature-based detection, anomaly-based detection, and/or stateful protocol analysis to detect and prevent network attacks against services or data-driven attacks on applications. Network security devices that provide application intermediary or proxy services on behalf of the network or applications are considered to be Application Layer Gateways (ALGs) and are out of scope for this SRG.

SRG requirements must be considered depending on the specific implementation of the IDPS and the location of the installation (i.e., regional enclave, enterprise data center, or local network). IDPS functions also can be included in other network devices, such as firewalls. If other functions are implemented by the IDPS, the security requirements for that functionality must also be applied using additional SRGs and/or STIGs. Configuration of the operating system, any non-integrated database logging application, non-integrated analysis tools, and network device management are covered by applicable SRGs.

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 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 IDPS SRG is based on the Network SRG. This IDPS 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}-{6-digit numeric sequence number}

Examples:

SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
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. TECHNOLOGY OVERVIEW

This section provides background information on IDPS devices 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 this technology or DoD network architecture. Focus is placed on providing an understanding of the types of products covered within the scope and the associated security considerations. This background gives supplementary information to help understand terminology used in the SRG.

3.1 Introduction

The network Intrusion Detection System (IDS) is an application that automates the intrusion detection process. Intrusion Prevention System (IPS) applications have all the capabilities of an IDS, but can also take action to stop a detected event. IDS and IPS applications offer many of the same capabilities, and administrators can usually disable prevention features in IPS products, causing them to function as an IDS. Accordingly, the term IDPS refers to both IDS and IPS technologies.

3.2 IDPS Components

The IDPS implementation consists of multiple components working together to provide traffic monitoring and prevention, including multiple sensors, management server/consoles, event analyzers, and management tools.

Sensors monitor and analyze network traffic for known and potential incidents based on various detection methodologies. Sensors include network-based, wireless, and network behavior analysis technologies. These sensors are placed at the perimeter and at key points in the internal infrastructure, depending on organizational architecture.

A management console (also called a management server) is a centralized device that receives information from the sensors and manages them. Some management servers and anomaly detection tools perform rate-based, data mining, and statistical analysis on the event log information collected from multiple sensors. These components can detect complex incidents such as distributed, command sequence, or injection attacks.

3.2.1 Detection Methods

To be effective in a complex environment such as DoD, IDPS implementations must use different methods to detect security incidents. No one detection method is effective for detecting all possible incidents. Thus, the organization’s intrusion detection and prevention solution must include IDS and IPS devices configured using a combination of signatures, rules, statistical analysis (known as anomaly detection), and security policy. These methods of intrusion detection work together to detect both known and unknown attacks and to implement organizational security policy. Since these terms are often used in a confusing manner, it is important to define how the IDPS SRG uses these terms to establish requirement.

A signature database contains definitions of predefined attack objects and groups. Traditional methods for intrusion detection are based on extensive knowledge of known attacks provided by experts. The signature database must be revised for each new type of intrusion that is discovered. A significant limitation of signature-based methods is that they cannot detect zero-day (i.e., new) attacks. Signature files are provided by vendors or other trusted sources and must be kept current to guard against newly discovered attacks or alterations to known attacks. Thus, once a new attack is discovered and its signature developed, there is some latency for the deployment and integration of the files into each system.

Signatures can be either atomic or stateful. Atomic signatures trigger on a single event, but do not require the system to maintain session state. These signatures consume minimal resources (such as memory) on the IDPS device. These signatures are easy to understand because they search only for a specific event. Atomic attack signatures look at single packets and are ideal for scanning for known attacks where state information (tracking established connections) is not necessary to identifying the specific attack. Unlike atomic signatures, stateful signatures trigger on a sequence of specific events that requires the IPS device to maintain state. Stateful signatures support stateful protocol analysis. Stateful protocol analysis involves performing protocol analysis for an entire connection or session, capturing and storing certain pieces of relevant data seen in the session, and using that data to identify attacks that involve multiple requests and responses.

The term rule is often used interchangeably with signatures, but generally refers to stateful signatures. Rules are often a composition of atomic signatures and can detect more complicated attacks and variants of known attacks. Rules are most often vendor-provided; however, some systems allow the creation of locally developed rules configured to match certain site or system-specific conditions.

With the increasing sophistication of attacks, signature- and rule-based intrusion detection methods have proven inadequate to detect sophisticated attacks, such as distributed attacks. Implementing IDPS devices that leverage anomaly-based detection techniques that use data mining and statistical analysis is imperative. These devices learn normal traffic patterns and compare current traffic patterns to detect possible incidents. Anomaly-based detection can detect incidents that may not be triggered by a standard rule or signature. Anomaly detection and protocol anomaly detection are both forms of stateful inspection. Protocol anomaly or protocol compliance inspections examine network traffic for unusual use or non-compliant use of protocols. Protocol anomaly detection includes the detection of bit flipping, buffer overflow, and command sequence attacks.

3.2.2 Next-Generation Application-Aware Technologies

Next-Generation IPS is a term coined by Gartner, Inc in the paper “Defining Next-Generation Network Intrusion Prevention,” by John Pescatore and Greg Young, Oct 7, 2011. This term has been rapidly adopted by major IPS vendors who are now selling products that significantly change the capabilities of network monitoring and prevention devices. At a minimum, a Next-Generation IPS will have standard First-Generation IPS capabilities and application awareness,

context awareness, and content awareness, especially those providing full stack inspection. With protocol-based inspection, these products provide protection against sophisticated attacks such as zero-day and DDoS attacks. These products also have application visibility, integrated threat context (stateful), reputation-based protection, behavior-based threat analysis and advanced malware detection. Some of the requirements within the SRG may only be met using a Next-Generation IPS product, which is often capable of performing functions that were previously reserved for routers and firewalls.

3.3 User Account Management

Accounts used with the IDPS implementation are privileged accounts. Non-privileged account management is out of scope. Additionally, the use of account information as part of the traffic monitoring, detection, and prevention functions is similarly out of scope. Privileged accounts created and maintained on authentication, authorization, and accounting (AAA) devices (e.g., RADIUS, LDAP, or Active Directory) are secured using the applicable security guide or STIG. Privileged accounts are secured using the NDM SRG.

3.4 Audit Logs Versus Sensor Logs

There are two types of log files required for each component of the organization's IDPS implementation, audit logs and sensor logs. The audit log stores the results of enforcement actions based on the access control restrictions, use of user privileges, and other security policies. This type of functionality is usually performed by the OS or device management functions of the network device. The sensor log stores events detected as part of the IDPS monitoring activity. Logs from multiple sensors must be combined in a centralized database server or syslog, depending on the implementation.

DoD requires audit logs be stored on a central logging server that aggregates audit logs; therefore many of the audit requirements are not part of the IDPS SRG scope. However, the IDPS implementation must also have the capability to centralize the sensor logs. Security requirement for the audit logs are in the NDM SRG while security requirements for the sensor logs are in the IDPS SRG.