APPLICATION LAYER GATEWAY (ALG) SECURITY REQUIREMENTS GUIDE (SRG) TECHNOLOGY OVERVIEW

Version 1, Release 2

24 July 2015

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

This 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. These devices, regardless of capability, are collectively referred to as Application Layer Gateways (ALGs) throughout the SRG.

The scope of this document includes Application Layer Gateways (ALG) and application-aware firewalls. These devices employ application proxies to provide intermediary services and/or to provide traffic filtering as traffic crosses key internal boundaries or as communications travel between different security domains. The SRG scope does not include coverage of devices or proxies that solely provide non-security network services, such as caching or load balancing, although these functions are often provided as part of ALGs and application-aware firewalls.

The terminology of products offered by vendors varies greatly. An attempt has been made to identify where these devices fit based on common functions provided by these devices rather than marketing terminology. A further complication is that products often combine functions so that customers may choose to turn on or add functions based on their mission needs and the desired network architecture. Thus, a product marketed as an application gateway may also provide content filtering. There are also many types of applications and application intermediary services, making these products difficult to categorize. ALGs and application firewall products can vary greatly in terms of specific functions provided.

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 those originating in Department of Defense (DoD) Instruction (DoDI) 8500.2 and 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 ALG SRG is based on the Network SRG. This ALG 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 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 ALG and application firewall 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 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

A gateway acts as an intermediary or interface between different enterprises, subnetworks, or security boundaries (e.g., internal network to the Internet). With an application proxy installed, today's gateways can provide application intermediary and/or content filtering on behalf of specific applications (e.g., web server, database, or email). These gateways translate transmitted communications from an endpoint and route the communications traffic to a host or destination (e.g., Internet). However, gateways also often perform common firewall tasks such as forwarding, restricting, blocking, or, increasingly, content filtering. By leveraging the installed application proxy, these capabilities can be done at the application layer, thus detecting and preventing more sophisticated attacks than traditional network firewalls.

A firewall blocks, filters, or restricts communications traffic as it crosses different enterprises, subnetworks, or security boundaries. When an application proxy is installed, today's firewalls can provide application content filtering, Network Address Translation (NAT), and/or proxy services. Application firewalls are advanced intelligent firewalls that can defend against and mitigate multiple threats, including those at the OSI application layer. To increase effectiveness, an application firewall is often incorporated into an application gateway at key security boundaries.

Gateways and firewalls, with the capability to provide intermediary and content filtering up to and including the OSI application layer, are most often referred to as application layer gateways and application firewalls. Common types of these advanced gateways and firewalls include the following:

- Application Layer Gateway (ALG)
- Web Application Firewall (WAF)
- Database firewall
- Web content filter
- Session Border Controller (SBC)
- Secure Sockets Layer (SSL) proxy
- Email gateway
- Authentication gateway
- Cross Domain Solution (CDS)

Installation of these products does not negate the DoD requirement for traffic inspection by a perimeter firewall and an Intrusion Prevention System (IPS).

3.2 Proxy Servers

Proxy servers are popular mechanisms for applying rules that restrict inbound and outbound network transmissions. A proxy server acts as an intermediary between the clients and external networks, including the Internet. The term proxy can be confusing since the configuration, services provided, and installation can vary widely.

Use of the term proxy in today's networking environment can be extremely confusing. Many devices contain proxies but do not fall within the scope of this SRG. For example, Virtual Private Networks (VPNs) often include one or more application proxies but are not considered proxy servers. Additionally, because of its ability to intercept (broker) messages entering and leaving the network, the proxy can be used to provide NAT where the internal network source and destination addresses of the network traffic are hidden from the external network or server.

Proxy servers provide secure access from the Internet to an internal application or endpoint, such as an email or web server. To an outside user, the proxy server appears to be the email or application server. The proxy responds to external requests on behalf of the internal application or endpoint.

3.3 SSL Gateway

An SSL gateway server decrypts inbound SSL connections for the purpose of inspecting the traffic. Encrypted communications on the SSL port (443) flow through SSL proxies that redirect the unencrypted content to be inspected and controlled before entering or exiting the enterprise. The SSL gateway can be deployed to protect enterprise resources from threats originating over SSL-based VPNs and other applications. An encryption key for the SSL VPN or SSL application is maintained in the SSL gateway and is used to decrypt, inspect, and forward packets

SSL has become the most widely used protocol for encryption of inbound and outbound network traffic. It provides data security for remote and mobile access across a public network and is also used to provide internal traffic separation. While SSL ensures end-to-end privacy, this encrypted traffic cannot be read by IPS and other network security devices. Encryption packets may contain malware, viruses or unauthorized commands that, once reaching its destination, can be harmful to internal and external networks and endpoints. Moreover, encryption makes identifying accidental or intentional leakage of confidential information difficult.

3.4 Application Layer Gateway (ALG)

Application layer gateways and application level firewalls are advanced firewalls that combine lower layer content filtering and traffic restrictions with OSI Layer 7 (Application Layer) functionality. In an application firewall, two connections are established: one between the traffic source and the firewall, and another between the firewall and the destination. Application firewalls contain proxy services that intercept arriving traffic on behalf of the destination, examine application payload, and then relay permitted traffic to the destination. The technology of an application firewall does not require network layer routes between the firewall interfaces.

The application firewall software performs the routing; thus, packets that traverse the firewall must do so under software control. Application firewall implementations can offer very granular application-level control (e.g., blocking file transfers involving executable files with names ending in .exe).

Advantages also include capabilities to enforce user authentication, hardware or software token authentication, source address authentication, and biometric authentication. However, due to full packet awareness, application firewalls have the potential to degrade high bandwidth or real-time solutions. These gateways also tend to be limited for new applications and protocols and can become capable of tunneling the new applications in a vendor-generic proxy agent. These generic proxy agents tend to negate many strengths of the application gateway.

3.5 Authentication Gateway

An authentication gateway provides centralized authentication services by acting as an intermediary between end-point devices and enterprise applications. The gateway can accept various forms of authorized credentials and work with multiple directory services to authenticate the end user. A centralized authentication gateway enables applications to leverage strong multi-factor authentication, such as PKI, without the need to integrate this service into each application, thus providing a way to map user-presented credentials, such as a Common Access Card (CAC), to a format suitable for the application or service.

3.6 Cross Domain Solution (CDS)

A CDS is a gateway or controlled interface that uses a trusted operating system and enforcing a security policy to provide access to and/or transfer of data between different security domains. Supplementary guidance is provided in this SRG based on the CDS Overlay and NIST SP 800-53 guidance. This overlay identifies the security controls required to protect against threats and manage security risks presented when utilizing a CDS to connect security domains (i.e., domains with differing classification or sensitivity levels). However, each CDS must follow the DoD-required process of testing, baselining, and risk assessment to ensure the rigor and accuracy necessary to rely upon a CDS for cross domain security.

The CDS Overlay identifies three types of CDSs:

- Access – An Access CDS provides access to a computing platform, application, or data residing on different security domains from a single device.
- Transfer – A Transfer CDS facilitates the movement of data between information systems operating in different security domains.
- Multi-level – A Multi-level CDS uses trusted labeling to store data at different classifications and allows users to access the data based upon their security domain and credentials.

Applicability of security controls varies based upon CDS type because of the differences in technical and operational constraints and associated interconnection risks. This SRG is designed to be used in conjunction with the latest version of the CDS Overlay, NDM SRG, OS SRG, and any applicable policy or architecture guidance.

3.7 Application Aware Firewalls

A firewall may be designed to operate as a filter at the level of IP packets or may operate at a higher protocol layer. Advances in network infrastructure engineering and information security have resulted in a blurring of the lines that differentiate the various firewall platforms. Unlike packet filter or stateful inspection firewalls, which simply look at the port and source and destination IP address, firewalls that support the application layer filtering feature have the ability to inspect the data and the commands being passed back and forth. Deep Packet Inspection (DPI), application-aware firewalls, Next Generation (Nextgen), and application firewall are some of the new terms used to describe content filtering technologies that examine network traffic for conformance, malware, and anomalies at higher layers of the OSI model.

Application-aware firewalls using deep packet inspection operate at Layer 4 of the OSI model with added enhancements to stateful inspection technology. Attacks can traverse a traditional stateful firewall even if the firewall is deployed and working normally. By adding application-oriented checking logic into processing modules, essentially merging signatures into the firewall traffic-processing engines of products, the firewall industry increased the depth of protection against worms, Trojans, email viruses, and exploits against software vulnerabilities. Deep packet inspection uses an attack object database to store protocol anomalies and attack patterns (sometimes referred to as signatures), grouping them by protocol and security level (severity). Packet processing is typically described as performing application-level checks as well as stateful inspection. The primary limitation of the technology is that it generally cannot detect threats that require many packets to transmit across the Internet.

Web Application Firewalls (WAFs) are designed to protect web applications from web-based attacks. This protection is similar to an inline IPS, but the WAF is highly specialized to provide deep analysis and content filtering of web application behavior and specific session requests and responses. WAFs protect against web application threats, such as SQL injection, cross-site scripting, session hijacking, parameter or URL tampering, and buffer overflows. Similar to other application firewalls, WAFs are typically deployed as a proxy, placed inline before the web application server or clients. This placement avoids the need for all network traffic to flow through the WAF.

Database firewalls alert or block database attacks and abnormal access requests in real time to protect against database attacks, including SQL injection, Buffer overflow and Denial of Service. They enable the systems administrator to create custom rules by specifying the type of the rule (Query Groups or Table Based), source IP address(es), database user(s), application name(s), schedule, and patterns or conditions where a query will be blocked, allowed, or monitored. The systems administrator can also enable or disable caching per policy.

3.8 User Account Management

Accounts used with the ALG 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 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.

3.9 Audit Logs versus Application Logs

There are two types of log files required for each component of the organization's ALG implementation, the audit log and sensor log(s). 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(s) store events detected as part of the ALG 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 ALG SRG scope. However, the ALG 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 log are in the ALG SRG.