

UNCLASSIFIED



SYMANTEC PROXY SECURITY GATEWAY (SG) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

24 January 2020

Developed by Symantec and 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 DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Executive Summary	1
1.2 Authority	1
1.3 Vulnerability Severity Category Code Definitions	1
1.4 STIG Distribution.....	2
1.5 SRG Compliance Reporting.....	2
1.6 Document Revisions	2
1.7 Other Considerations	2
1.8 Product Approval Disclaimer.....	3
2. ASSESSMENT CONSIDERATIONS.....	4
2.1 Security Assessment Information	4
2.1.1 Audit Logging.....	4
3. CONCEPTS AND TERMINOLOGY CONVENTIONS	5

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2

1. INTRODUCTION

1.1 Executive Summary

The Symantec ProxySG Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems and consists of the Symantec ProxySG Application Layer Gateway (ALG) STIG and the Symantec ProxySG Network Device Management (NDM) STIG. This document is meant for use in conjunction with other STIGs such as Network Infrastructure.

The Symantec ProxySG ALG STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the ProxySG appliance at the functional level.

The Symantec ProxySG NDM STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the management functions and backplane.

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 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 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 CONSIDERATIONS

2.1 Security Assessment Information

The Symantec ProxySG ALG and NDM STIGs are meant for use in conjunction with other STIGs/SRGs such as Network Infrastructure STIG, AAA SRG, and Central Log Server SRG to ensure a complete security assessment is achieved.

2.1.1 Audit Logging

Symantec ProxySG has various types of audit logs that must be secured and inspected as part of a compliance inspection.

The event log captures information of anyone logging on to the device. This is a local file that can only be accessed via the web management console under Statistics.

The management control log is extremely granular and is not required under normal operational conditions. It is enabled by default and cannot be turned off.

The access log, which contains user activity logging, captures events related to traffic flow. It must be enabled and configured. See the ProxySG Administration Guide for more information on correctly configuring Access Logging for each rule.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

Symantec ProxySG is most often deployed in a forward web proxy architecture that monitors and filters outbound traffic. However, the device can also be deployed as a reverse web proxy that examines inbound traffic, such as requests from the Internet to access resources (servers) in a protected enclave (e.g., DMZ, private).

Security policies are assigned to devices or users who request access to network resources under purview of the proxy. These policies typically filter using the HTTP protocol and do content filtering based on the source or destination address space or domain name. Forward proxy installations typically rely heavily on reputation-based categorization of the source or destination domain (e.g., gambling, auction, advertisements, etc.), a native capability of the product. The product can be configured for both explicit (client is aware of the proxy) and/or transparent proxy (where the client is unaware that it is sending traffic to a proxy). Ideally, multiple web access layer security policies are combined to leverage DoD's required web restrictions. Connecting devices can also be assessed and restricted based on IP address, geolocation, and many other filters.

Symantec ProxySG can be combined with other functions such as content analysis, malware analysis, anti-virus analysis, and data loss prevention (DLP) to extend its security functions. Extended capabilities such as these work by examining the data within the packets at more granular levels, such as file inspection and signature-based malware detection. These functions are out of scope for this STIG effort. Organizations that choose to purchase and enable licenses for these extended features of any security device need to consider performance and bandwidth throughput impacts as a result of the additional overhead.

Symantec recommends most DoD sites also purchase a license for URL Threat Risk Levels. According to Symantec, "The Threat Risk Levels service assigns threat risk levels to URLs according to specific criteria." This product is also out of scope for this STIG since it is not part of the base purchase.