F5 BIG-IP
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

29 January 2024

Developed by DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 2
1.4 STIG Distribution 2
1.5 Document Revisions 2
1.6 Other Considerations 2
1.7 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 Security Assessment Information 4
2.2 BIG-IP Device Management Configuration 4
2.3 BIG-IP LTM STIG 4
2.4 BIG-IP APM STIG 4
2.5 BIG-IP ASM STIG 4
2.6 BIG-IP AFM STIG 4

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The F5 BIG-IP Security Technical Implementation Guide (STIG) provides security policy and technical configuration requirements for deploying the appliance in the Department of Defense (DOD) networking environment. The BIG-IP appliance provides integrated application delivery services that work together on the same hardware. These services include load balancing, SSL off-loading, access control, and application firewall services.

The F5 BIG-IP STIG includes the following:

- BIG-IP Device Management STIG.
- BIG-IP Local Traffic Manager (LTM) STIG.
- BIG-IP Application Security Manager (ASM) STIG.
- BIG-IP Access Policy Manager (APM) STIG.
- BIG-IP Advanced Firewall Manager (AFM) STIG.

The BIG-IP LTM provides traffic management for rapid deployment, optimization, load balancing, and off-loading of sessions between users and application servers. This module is the core for all deployments of the BIG-IP device, and all other modules are used to define profiles and policies that are applied to virtual servers defined in the LTM.

The BIG-IP APM protects public-facing application by providing secure, policy-based, and context-aware access control. It centralizes and simplifies authentication, authorization, and accounting (AAA) management and covers the Authentication Gateway Service (AGS) requirements to support Federated Single Sign-On (SSO).

The BIG-IP ASM is an advanced web application firewall that protects critical applications and their data by defending against application-specific attacks that bypass conventional firewalls. It protects applications with comprehensive, policy-based web application security that blocks attacks and scales to ensure performance.

The BIG-IP AFM is a high-performance, stateful, full-proxy network firewall designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols, including HTTP/S, SMTP, DNS, and FTP. By aligning firewall policies with the applications they protect, the BIG-IP AFM streamlines application deployment, security, and monitoring.

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.

1.3 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 **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 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. 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 Authorizing Official (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. 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 Security Assessment Information

The implementation of the F5 BIG-IP STIGs occurs in two parts. The implementation of the BIG-IP Device Management STIG is used for the configuration of the BIG-IP device. The STIGs for the LTM module, APM module, ASM module, and AFM module will be used for the configuration of the respective modules in handling user authentication and traffic management with respect to the application gateway services being provided by the BIG-IP device.

2.2 BIG-IP Device Management Configuration

The BIG-IP Device Management STIG is required for all BIG-IP implementations.

2.3 BIG-IP LTM STIG

The F5 BIG-IP LTM STIG is required for all F5 BIG-IP deployments and will incorporate the STIGs for the APM module, ASM module, and AFM module, depending on the application gateway services required for the deployment of the BIG-IP device. To implement the F5 BIG-IP LTM STIG, each requirement is evaluated based on the BIG-IP deployment. For requirements that require the configuration of additional modules within the BIG-IP, the checks and fixes will specify those modules. When the configuration of other modules is required to meet a requirement, the corresponding requirement in the applicable module STIG will be followed for check and fix actions.

2.4 BIG-IP APM STIG

The BIG-IP APM STIG will be implemented when the BIG-IP deployment uses authentication services. The BIG-IP APM STIG will be implemented in conjunction with the BIG-IP LTM STIG to manage authentication services for defined virtual servers.

2.5 BIG-IP ASM STIG

The BIG-IP ASM STIG will be implemented when the BIG-IP deployment performs application proxy services. The BIG-IP ASM STIG will be implemented in conjunction with the BIG-IP LTM STIG to manage application proxy services for defined virtual servers.

2.6 BIG-IP AFM STIG

The BIG-IP AFM STIG will be implemented in conjunction with the BIG-IP LTM STIG to manage application firewall services for defined virtual servers.