F5 BIG-IP 11.x
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

23 October 2020

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

The F5 BIG-IP 11.x Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to F5 BIG-IP device and modules.

The F5 BIG-IP STIG contains five (5) STIGs for configuring the BIG-IP device according to the configuration and purpose of the device. The following are the five STIGs included as part of the F5 BIG-IP STIG:

- 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

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.

1.3 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 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 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.

2. CONCEPTS AND TERMINOLOGY CONVENTIONS

2.1 Overview

The BIG-IP device is a system that 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. At a minimum, it is recommended that the BIG-IP device be deployed with the Local Traffic Manager (LTM) and Access Policy Manager (APM) modules.

2.2 BIG-IP Local Traffic Manager (LTM) Module

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.

2.3 BIG-IP Access Policy Manager (APM) Module

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).

2.4 BIG-IP Application Security Manager (ASM) Module

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.

2.5 BIG-IP Advanced Firewall Manager (AFM) Module

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.

3. GENERAL SECURITY REQUIREMENTS

3.1 Overview

The implementation of the F5 BIG-IP STIGs occurs in two (2) parts. The implementation of the BIG-IP Device Management STIG will be 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.

3.2 BIG-IP Device Management Configuration

To implement the F5 BIG-IP STIGs, administrator access is required to the BIG-IP system management console. For the purposes of interpreting this STIG, the BIG-IP Device Management STIG will be used for the configuration of access and management of the BIG-IP device.

To ensure that the F5 BIG-IP meets the requirements within the STIG, the F5 BIG-IP shell would be locked down to limit the ability to modify the configuration through the shell. The following commands would be performed as a shell prompt after accessing the F5 BIG-IP using SSH.

(tmos)# modify sys db systemauth.disableRootLogin value true
(tmos)# modify sys db systemauth.disablebash value true
(tmos)# save sys config

3.3 BIG-IP LTM Configuration

The F5 BIG-IP LTM STIG will be implemented 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 pertaining to 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.

3.4 BIG-IP APM Configuration

The BIG-IP APM STIG will be implemented when the BIG-IP deployment utilizes 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.

3.5 BIG-IP ASM Configuration

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.

3.6 BIG-IP AFM Configuration

The BIG-IP AFM STIG will be implemented when the BIG-IP deployment performs application firewall services. 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.