

UNCLASSIFIED



**F5 BIG-IP TRAFFIC MANAGEMENT OPERATING
SYSTEM (TMOS)
SECURITY TECHNICAL IMPLEMENTATION GUIDE
STIG OVERVIEW**

26 September 2024

Developed by F5 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 the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Executive Summary.....	1
1.2 Authority.....	2
1.3 Vulnerability Severity Category Code Definitions.....	2
1.4 STIG Distribution.....	2
1.5 Document Revisions.....	2
1.6 Other Considerations.....	3
1.7 Product Approval Disclaimer.....	3
2. ASSESSMENT CONSIDERATIONS.....	4
2.1 Security Assessment Guidance.....	4
2.2 FIPS License Operational Mode.....	4
2.3 BIG-IP Device Management STIG.....	4
2.4 BIG-IP ALG STIG.....	4
2.5 BIG-IP Firewall STIG.....	5
2.6 BIG-IP DNS STIG.....	5
2.7 BIG-IP VPN STIG.....	5

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2
Table 2-1: Security Assessment Based on Services.....	4

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, application delivery, SSL off-loading, access control, firewall, virtual private network (VPN), and name resolution services.

The F5 BIG-IP STIG includes the following:

- BIG-IP Network Device Management (NDM) STIG.
- BIG-IP Advanced Firewall Manager (AFM) STIG.
- BIG-IP Application Layer Gateway (ALG) STIG.
- BIG-IP Virtual Private Network (VPN) STIG
- BIG-IP Domain Name System (DNS) STIG.

The core technology for the BIG-IP appliance is the Traffic Management Operating System (TMOS) and logical software modules run within TMOS. Modules within the scope of this STIG include the Local Traffic Manager (LTM), Access Policy Manager (APM), AFM, Advanced Web Application Firewall (AWAF), and DNS.

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 BIG-IP deployments, 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 AFM is a stateful, full-proxy network firewall designed to guard data centers against incoming threats that enter the network. The STIG security requirements ensure firewall policies are implemented to monitor and secure the applications they are configured to protect. Depending on the organization's needs, users may prefer to put all active rules in a single policy applied at the global context or apply firewall policies for specific virtual servers. The latter allows for application-specific policies to be developed and applied only where required. When processing policies and rules on a virtual server, only those specific to the application are processed.

The BIG-IP AWAF is a 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.

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 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 Guidance

Security assessment for the BIG-IP occurs in two parts: An assessment of the device management and backplate functions, and a review of the security configuration as it pertains to the traffic flow. Security reviews will always consist of multiple STIGs depending on the role of the appliance in the enclave. At a minimum, all security reviews must include the NDM and ALG STIGs.

Additionally, the corresponding STIG for each licensed and provisioned TMOS module must also be included in the security assessment. The following sections discuss the applicability and requirement contents of each STIG.

Table 2-1: Security Assessment Based on Services

Licensed and Provisioned Services	NDM STIG	ALG STIG	Firewall STIG	DNS STIG	VPN STIG
Load Balancing	Required				
SSL Off-loading	Required	Required			
Application Proxy	Required	Required			
Access Control	Required	Required			
Firewall	Required	Required	Required		
IPsec VPN	Required	Required			Required
Name Resolution	Required	Required		Required	

2.2 FIPS License Operational Mode

The STIG requirements assumes that BIG-IP is installed in the FIPS Compliant Mode. The FIPS validated module activation requires installation of the license referred as “FIPS license”. When operated in the FIPS Compliant Mode, the BIG-IP inherently meets the STIG requirements for use of cryptographic modules that are FIPS 140-2 validated. FIPS Compliant Mode is required.

2.3 BIG-IP Device Management STIG

The BIG-IP NDM STIG is required for all deployments. This STIG contains requirements applicable to secure administrative access, logging, least privilege, account of last resort, and system control plane configuration. Some settings are also globally applicable to the licensed and provisioned TMOS modules.

2.4 BIG-IP ALG STIG

The BIG-IP ALG STIG is required for all deployments. This STIG covers security requirements for the LTM, APM, and AWAf. However, applicability of each STIG requirement depends on the modules and licenses used. The LTM is the base module for TMOS and is required in DOD for all customers. The APM and AWAf are separately licensed. In the ALG STIG, applicability of the requirement to each module is identified in the check and fix. The SSL VPN requires the APM

module since the access control lists are part of the APM; thus, the BIG-IP ALG STIG is required when using the SSL VPN functions.

2.5 BIG-IP Firewall STIG

In addition to the NDM and APM STIGs, the BIG-IP Firewall STIG is required when the AFM module is licensed and provisioned. It is a stateful full proxy network firewall. This STIG does not cover the AWAFF module.

2.6 BIG-IP DNS STIG

In addition to the NDM and APM STIGs, the BIG-IP DNS STIG is required when the DNS module is installed and provisioned. This module provides and proxies DNS services for clients.

2.7 BIG-IP VPN STIG

In addition to the NDM and APM STIGs, the BIG-IP VPN STIG is required when using the IPsec VPN in the LTM. The BIG-IP IPsec implements only site-to-site VPNs. The Firewall STIG is also required to ensure VPN traffic is monitored and logged.