FORTINET FORTIGATE FIREWALL SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

27 October 2022

Developed by Fortinet and DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Fortinet FortiGate Firewall Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with other STIGs such as the Enclave, Network Infrastructure, Secure Remote Computing, and appropriate operating system (OS) STIGs.

The Fortinet FortiGate is a next-generation firewall (NGFW), providing security-driven networking and consolidating security capabilities, such as; intrusion prevention, web filtering, SSL inspection, and automated threat protection.

The scope of this STIG document covers the device management and firewall features of the device in two separate STIG documents. Future versions of this STIG document may cover other features of the device.

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

	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 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 Controlled Unclassified Information (CUI) will be available for 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 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.

1.8 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). 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 FortiGate Firewall Security Readiness Review (SRR) ensures that the site has properly provisioned and implemented the device and it is being managed in a way that is secure, efficient, and effective. The STIG identifies vulnerabilities that undermine security in that they have the potential to affect the confidentiality, integrity, or availability of the device. The items reviewed are based on standards and practices published by the DOD, their contractors, and other security guidance entities, following guidance published in the DODI 8500.2 and National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 security controls.

DISA has assigned a level of urgency to each finding based on Chief Information Officer (CIO) established criteria for Certification and Accreditation (C&A). All findings are based on regulations and guidelines. All findings require correction by the host organization.

The NIST SPs in the 800 series are of general interest to the computer security community. This series reports on ITL's research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. The NIST 800 series SPs can be referenced at http://csrc.nist.gov/publications/PubsSPs.html.

NIST SP 800-53, which is publicly available, is titled "Security and Privacy Controls for Federal Information Systems and Organizations". The SP 800-53 provides information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines do not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

NIST SP 800-18, which is publicly available, is titled "Guide for Developing Security Plans for Federal Information Systems". The SP 800-18 provides both guidelines and a template for security plan creation and can serve as a base for development.

This document and the accompanying STIG provide the methods to assess vulnerabilities on deployed FortiGate Firewalls and perform a successful SRR.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Technology Description

NGFWs filter network traffic to protect an organization from internal and external threats and maintain features of stateful firewalls such as packet filtering, VPN support, network monitoring, and IP mapping features. NGFWs possess deeper inspection capabilities that give them a superior ability to identify attacks, malware, and other threats and provide organizations with application control, intrusion prevention, and advanced visibility across the network.