VMWARE NSX-T DATA CENTER SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

26 July 2023

Developed by VMware and DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, Quality-of-Service [QoS]) in software. As a result, these services can be programmatically assembled in any arbitrary combination to produce unique, isolated virtual networks.

NSX-T Data Center works by implementing three separate but integrated planes: management, control, and data. The three planes are implemented as a set of processes, modules, and agents residing on three types of nodes: manager, controller, and transport.

The VMware NSX-T 3.x Security Technical Implementation Guides (STIGs) provide security policy and technical configuration requirements for the use of NSX-T 3.x in the Department of Defense (DOD). The VMware NSX-T 3.x STIG comprises the following individual STIGs:

- VMware NSX-T 3.x Manager STIG.
- VMware NSX-T 3.x SDN Controller STIG.
- VMware NSX-T 3.x Distributed Firewall STIG.
- VMware NSX-T 3.x Tier-0 Gateway Router STIG.
- VMware NSX-T 3.x Tier-0 Gateway Firewall STIG.
- VMware NSX-T 3.x Tier-1 Gateway Router STIG.
- VMware NSX-T 3.x Tier-1 Gateway Firewall STIG.

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

VMware NSX-T 3.x includes a number of components and capabilities, each requiring separate STIG coverage. NSX-T capabilities can be used in a variety of architectures and implementations; however, the minimum required documents are the NSX-T 3.x Manager and SDN controller STIGs.

Additionally, because NSX-T has networking capabilities beyond what is covered in these STIGs, a complete security assessment requires assessing all capabilities and functions used in the specific DOD implementation. Examples include securing the Hypervisor, servers/hosts, and AAA services. Because product STIGs are not available for all capabilities, use of existing generic technology STIGs may be required to secure these functions.

Support for DOD CAC is required for access to network implementations. Currently, use of VMware Identity Manager (vIDM) or Workspace ONE Access are the only solutions approved for use with VMware NSX-T. Depending on which of these two identity and access management solutions is chosen, the applicable supplemental documentation provided with this STIG must be used as a configuration guide. These documents were developed and provided by the vendor to support DOD clients.

The following STIGs have been developed for NSX-T 3.x:

- VMware NSX-T 3.x Manager STIG – This STIG must be used to enhance the security configuration of the NSX-T Manager that provides the management plane capabilities of NSX-T.
- VMware NSX-T 3.x SDN Controller STIG – As of NSX-T 2.4, the Manager and Controller functionality are cohosted on the same appliance and deployed as a cluster of three nodes. While the VMware NSX-T 3.x Manager STIG covers many of the requirements for this appliance, a few unique requirements in the SDN Controller SRG are covered in this STIG.
- VMware NSX-T 3.x Distributed Firewall STIG – This STIG must be used to enhance the security configuration of the NSX-T Distributed Firewall capability, which provides a centrally controlled but operationally distributed firewall that is attached directly to workloads. If enabled, this service is installed on a hypervisor, which must be STIG compliant using the applicable STIG.
- VMware NSX-T 3.x Tier-0 Gateway Router STIG – The VMware NSX-T 3.x Tier-0 Gateway Router STIG must be used to enhance the security configuration of the NSX-T Tier-0 Gateway Router capability.
- VMware NSX-T 3.x Tier-0 Gateway Firewall STIG – This STIG must be used to enhance the security configuration of the NSX-T Tier-0 Gateway Firewall capability.
- VMware NSX-T 3.x Tier-1 Gateway Router STIG – This STIG must be used to enhance the security configuration of the NSX-T Tier-1 Gateway Router capability.
- VMware NSX-T 3.x Tier-1 Gateway Firewall STIG – This STIG must be used to enhance the security configuration of the NSX-T Tier-1 Gateway Firewall capability.