Configuring NSX for Common Criteria

NSX for vSphere 6.3

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

VERSION-02- MAR 31, 2017

vmware

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.

3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

List of Tables

1.0 Configuring NSX for Common Criteria

Overview

The Configuring NSX for Common Criteria document provides guidance on the secure installation and secure use of the Target of Evaluation (TOE) for the Common Criteria Evaluation for the VMware® NSX™ product.

This document provides clarifications and changes to the VMware documentation listed in the Document References section, and should be used as the guiding document for the installation and administration of the TOE in the Common Criteria evaluated configuration. The official VMware documentation should be referred to and followed only as directed within this guiding document.

This document is based on the VMware NSX for vSphere 6.3 Common Criteria (CC) documentation suite that address the requirements of the Evaluation Assurance Level (EAL) 2+ (ALC_FLR.1).

Note: This is not the official Common Criteria (CC) Guidance document.

For official CC documents, visit VMware Common Criteria Evaluation & Validation Page.

Intended Audience

This information is intended for VMware® NSX™ customers, and the VMware development staff.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Here is the list of terms used in this document:

- CC: Common Criteria
- EAL: Evaluation Assurance Level
- TOE: Target of Evaluation

Common Criteria (CC) Identifiers

Table 1: Identifiers displays the Target of Evaluation (TOE), version of CC and assurance component addressed in this document.

Table 1: Identifiers

Item	Detail

TOE	VMware NSX for vSphere 6.3
CC version	3.1R4
Assurance components	AGD_PRE.1

Document References

Table 2: References provides the list of relevant reference documents. You can find the latest NSX documents at NSX for vSphere 6.3 Documentation Center.

Table 2: References

Reference Number	Document
A	VMware NSX for vSphere 6.3 Security Target – Version 2.4
B	VMware NSX for vSphere 6.3 Administration Guide
C	VMware NSX for vSphere 6.3 Troubleshooting Guide
D	VMware NSX for vSphere 6.3 API Guide
E	VMware NSX for vSphere 6.3 Command Line Interface Reference
F	VMware NSX for vSphere 6.3 Installation Guide
G	VMware NSX for vSphere 6.3 Cross-vCenter Installation Guide
H	VMware NSX for vSphere Hardening Guide - Version 1.6
I	Self-Service Download Maintenance Tool Quick Reference Guide - Version 1.8

You can find the latest NSX documents at NSX Documentation Center and at VMware NSX Communities Page.

Evaluated TOE Configuration

- **NSX Security Target Document**: The evaluated TOE configuration is as described in this document. The evaluated configuration includes details on assumptions, security policies, and parameters for configuration, and should be used in conjunction with this document.
- **NSX Installation Guide**, **NSX Cross-vCenter Installation Guide**, and **NSX Hardening Guide**: Use *NSX Installation Guides* to ensure all TOE evaluation configurations are applied in the end user environment.

  Installation procedures detailed in these guides should be used to install and configure the TOE.

  Applicable sections are dependent on the end user environment, and must be in accordance with parameters specified in *NSX Security Target* document.

2.0 Guidance

The following guidance steps in this section of the document must be followed to maintain the evaluated configuration of the TOE.

Enabling SSH

NSX Manager, NSX Edge, and NSX Controller have standard SSH interfaces, through which SSH clients can connect to in order to execute command line functions securely. The NSX Edge and NSX Controller versions of SSH implemented by the TOE have a known vulnerability that, if exploited, could result in a denial of service to the SSH communications channel. For this reason, SSH should not be enabled for external communications.

Note: By default, SSH is disabled. If you want to SSH, you can use the vSphere console for accessing equivalent CLI commands.

To disable SSH for NSX Controller, refer to *NSX Hardening Guide*.

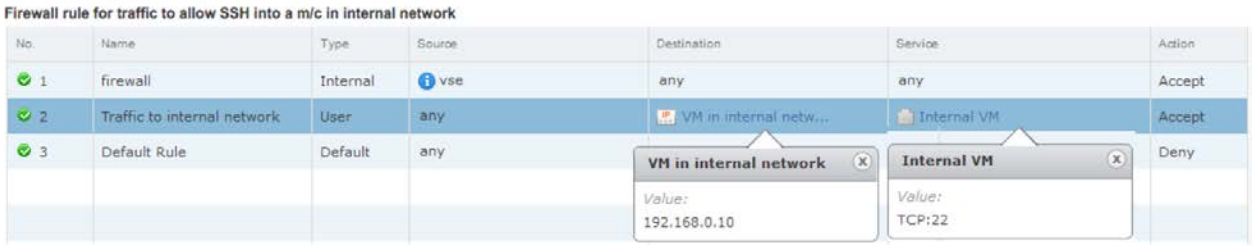
For internal communications, where administrators are trusted, enabling SSH is permitted.

You can enable or disable SSH for NSX Manager using Command Line Interface (CLI). For CLI details, refer to *NSX Command Line Interface Reference*.

To enable SSH for NSX Edge, refer to the **Routing** section in the *NSX Administration Guide*. Administrators should also configure a firewall rule that permits the information flow for the SSH channel. Refer to **Working with Firewall Rules** section in the *NSX Administration Guide* for a general understanding of firewall functionality. Online documentation provides detailed instructions for firewall configuration.

Latest NSX documents are available at NSX Documentation Center.

The following configuration should be applied:



You can enable or disable SSH for NSX Edge using API. For API details, refer to *NSX API Guide.*

FIPS Mode

To configure cryptographic functionality of the TOE to be in accordance with the *NSX Security Target* document, Administrators need to enable FIPS mode.

By default, FIPS mode will be turned off in NSX Manager. (FIPS mode in OpenSSL is ON and for RabbitMQ broker, FIPS mode is OFF). This feature ensures that when you upgrade NSX Manager from

any version lower than 6.3.x, communication between NSX Manager and other components remains available during the upgrade process.

You can enable/disable FIPS mode from NSX Manager virtual appliance. For details refer to **Change FIPS Mode and TLS Settings on NSX Manager** topic in the *NSX Administration Guide.* You must navigate to NSX Manager virtual appliance as an immediate priority upon installation.

Alternatively, FIPS mode can be enabled using the REST API as follows:

```
POST https://<nsxmgr-ip>/api/4.0/edges/{edgeId}/fips?enable=true|false
```

Note that all NSX REST API requests require authorization. For details, refer to **Using the NSX REST API** topic in the *NSX API Guide*.

Cryptographic Guidance

To securely operate the TOE with FIPS 140-2 validated cryptographic modules, ensure that:

- The TOE is installed and configured in FIPS mode, as per FIPS Mode section of this document, and
- Only those cryptographic algorithms and parameters specified in **Section 5** of *the VMware NSX for vSphere 6.3 Security Target* document are used for configuration.

3.0 Exclusions and Environment

1 Only those features and functions described in the *VMware NSX for vSphere 6.3 Security Target* document should be included in a VMware NSX for vSphere 6.3 evaluated installation for TOE components described.

2 Additionally, the TOE operates with the following components in the environment:

a) **Anti-virus and anti-malware services.** These are provisioned by third parties.

b) **Audit Server.** The TOE can utilize a Syslog server to store audit records. Configuration of an audit server is at user discretion.

c) **Web Browser.** The remote administrator can use a web browser to access the vSphere Web Client interface.

d) **Domain credential authorization.** This is outside of scope and is at the discretion of the user for configuration options.

e) **NTP Time Server**.

f) **All physical installation media**.

Unevaluated NSX Features

You can view the functionality difference between FIPS mode and non-FIPS mode in **FIPS Mode** section in the *NSX Administration Guide.*

The following features are not included in the VMware NSX for vSphere 6.3 evaluated installation for TOE components.

- **IPSec VPN** –Refer to the **IPSec VPN Overview** section in the *NSX Administration Guide.*
- **Controller ToR** - If you have a hardware gateway (hardware VTEP) installed in your environment, upgrade to NSX 6.3.0 is blocked. You must contact VMware support to proceed with the upgrade. See VMware Knowledge Base article 2148511 for more information.
- **SSL VPN Windows Certificate Authentication** – For information and steps on adding certificate-based client authentication for Windows SSL VPN-Plus clients, see VMware Knowledge Base article 2147978 .

4.0 Additions

The following additions must be addressed in order to fully comply with the TOE Security Policy.

Authentication and Password Security

Upon installation of the TOE in accordance with *NSX Installation Guide*, the TOE (NSX Manager) will prompt the user to specify a password for the admin account during the installation or upgrade procedure. There is no programmatic checking of password complexity requirements. As such, to adequately protect the TOE from unauthorized use, administrators are required to adhere to and enforce a password policy that contains the following rules:

- Minimum password length of eight (8) characters.
- At least one number, one uppercase letter, one lowercase letter, and one special character must be included.
- Dictionary words are not permitted to be part of the password.
- The password cannot contain three or more subsequent characters from the user's account name.