Fortanix®

Administration Guide

FORTANIX DATA SECURITY MANAGER – PORT REQUIREMENTS

VERSION 2.0

Fortanix Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | United States of America | ☎ +1 (650) 943-2484 |
✉ info@fortanix.com | 🌐 www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 PURPOSE

Welcome to the Fortanix Data Security Manager (DSM) Administration guide. The purpose of this guide is to describe the Fortanix DSM port requirements.

1.2 INTENDED AUDIENCE

This setup guide is intended to be used by technical stakeholders of Fortanix DSM who will be responsible for planning, performing, or setting up the monitoring and alerting solution, such as the Systems Administrator, Chief Information Officer (CIO), Analysts, or Developers.

2.0 LIST OF REQUIRED OPEN PORTS

The following table describes what needs to be in place before the Fortanix DSM can be deployed.

2.1 EXTERNAL/APPLICATION PORTS

The following ports need to be accessible by clients wanting to access Fortanix DSM.

PROTOCOL	INBOUND / OUTBOUND	PORT NUMBER	LOAD BALANCER USE (YES/NO)	PURPOSE
TCP	Inbound	22	No	SSH connection to DSM server
TCP	Inbound	443	Yes	HTTPS – Used for WebUI and calling REST API. Applications will access cluster URL on this port. Each individual node will also need this port open.
TCP	Inbound	4445	Yes	HTTPS - Used for delivering static content in WebUI.
TCP	Inbound	5696	Yes	Used by applications that use KMIP for interacting with Fortanix DSM. Applications will access cluster URL on this port. Each individual node will also need this port open.

2.2 INTRA-CLUSTER PORTS

The following ports are needed for communication between different cluster nodes.

PROTOCOL	INBOUND / OUTBOUND	PORT NUMBER	LOAD BALANCER USE (YES/NO)	PURPOSE
IP			No	Protocol Number 112 (VRRP) – Cluster IP negotiation (keepalived)
TCP	Both	2379	No	HTTP – etcd API (This port uses TLS after upgrade to 3.24)
TCP	Both	2380	No	etcd intra-cluster communication
TCP	Both	2382	No	etcd intra-cluster communication over TLS (This port needs to be open before upgrading to 3.24)
TCP	Both	6443	No	HTTPS – Kubernetes API
TCP	Both	10250	No	Kubelet Port
UDP	Both	8472	No	VXLAN – intra-cluster communication

2.3 OUTBOUND PORTS

The following outbound ports must be open for Fortanix DSM in case these external systems shall be accessible.

PROTOCOL	INBOUND / OUTBOUND	PORT NUMBER	LOAD BALANCER USE (YES/NO)	PURPOSE
TCP	Outbound	SMTP	No	If SMTP email is configured
TCP	Outbound	443	No	If email is configured using AWS SES
UDP	Outbound	514	No	if external Syslog is used with fluentd configuration for cluster POD logs
TCP	Outbound	514	No	if external syslog is used to push Audit logs

PROTOCOL	INBOUND / OUTBOUND	PORT NUMBER	LOAD BALANCER USE (YES/NO)	PURPOSE
TCP	Outbound	514	No	If external logging using syslog TLS is configured
TCP	Outbound	8089	No	If external logging using Splunk is configured
TCP	Outbound	443	No	If external logging using Google stack driver is configured
TCP	Outbound	636	No	If SSO authentication with AD/LDAP is configured
TCP	Outbound	443	No	If external logging using OAuth is configured
TCP	Outbound	443	No	For connection to IAS proxy if attestation is enabled
UDP	Outbound	123	No	When external NTP is configured.
TCP	Outbound	80	No	Used for Intel remote attestation when SGX is configured. For more details refer to the Fortanix DSM Attestation Guide.
TCP	Outbound	443	No	Used for Intel remote attestation when SGX is configured. For more details refer to the Fortanix DSM Attestation Guide.
TCP	Outbound	443	No	Used for communication with GitHub repository for Fortanix DSM plugins. *Refer to https://github.com/fortanix/sdkms-plugin-library*
TCP	Outbound	53	No	The DNS ports that are used to query and request information from the DNS servers.
UDP	Outbound	53	No	The DNS ports that are used to query and request information from the DNS servers.

2.4 MANAGEMENT INTERFACE PORTS

When the MGMT network port is connected to the network, the following ports must be open to use the Intelligent Platform Management Interface (IPMI);

PROTOCOL	INBOUND / OUTBOUND	PORT NUMBER	LOAD BALANCER USE (YES/NO)	PURPOSE
TCP	Inbound	80	No	Only applicable for FX2200 appliances - For IPMI WebUI
TCP	Inbound	443	No	Only applicable for FX2200 appliances - For IPMI WebUI via HTTPS if configured
UDP	Inbound	623	No	Only applicable for FX2200 appliances - For IPMI and SOL

3.0 DOCUMENT INFORMATION

3.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/360052751791-Fortanix-Data-Security-Manager-Port-Requirements

3.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com