# MSLA Product Terms

## Cisco Secure Firewall Threat Defense Virtual

## (formerly Next-Generation Firewall Virtual)

**Additional Product Terms**

Service Provider's use of Cisco Secure Firewall Threat Defense Virtual, formerly Next-Generation Firewall Virtual, under the MSLA Program Terms is subject to these Product Terms. These terms take precedence over any conflicting terms in the Program Terms. Capitalized terms used but not defined in these Product Terms are defined in the Program Terms or the Master Agreement. For purposes of these Product Terms, Cisco Secure Firewall Threat Defense Virtual is referred to as "Secure Firewall."

**Product Description**

Secure Firewall offers threat protection features and centralized management, resulting in consistent security effectiveness and visibility across physical and virtual workloads. It is available in multiple performance tiers and includes the following in each tier.

*Base Subscription*: The base subscription includes application visibility and control to reduce the potential surface area of attacks through granular control of thousands of applications. Secure Firewall enforces mobile, social, and other acceptable use policies. Your Secure Firewall subscription also includes access to the SecureX Cloud Service, Cisco's cloud-based, integrated security platform that aggregates threat intelligence, unifies visibility across various Cisco and third-party security products, enables automated workflows, and more.

*Optional Add-On Subscriptions*:

- **Threat Subscription:** Includes IPS, which allows Service Provider to perform intrusion detection and prevention, file control, and security intelligence filtering.
- **Malware Subscription:** Consists of Malware Defense for Cisco Secure Firewall (formerly AMP Ecosystem for Networks) and protects against sophisticated, targeted, zero-day, and persistent advanced threats. Malware Defense is a Cloud Service that continuously analyzes Files and network traffic for threats that evade End User's first lines of defense. It provides advanced malware analysis and protection solution that allows Service Provider and its End Users to conduct metadata File analysis to detect malware and cyber threats. Cryptographic hashes of files are collected and transmitted to a Cisco-managed cloud server where File reputation analysis is performed, and a disposition is made as to whether the File is good, bad, or unknown. After the File analysis is completed, Malware Defense will act on the disposition (e.g., by deleting the File and putting it into quarantine if it is determined to be malicious).
- **URL Filtering Subscription:** Allows Service Provider to write a condition in an access control rule to determine the traffic that traverses a network based on non-encrypted URL requests by the monitored hosts.

**1. Supplemental Terms**

**1.1. Versions**. Service Provider's use of Next Generation Firewall Virtual MSLA Software (SPLA-NGFWV-PKG-M) is limited to version 6.3 or higher. Service Provider's use of Secure Firewall Threat Defense Virtual MSLA Software (MSLA-FTDVSEC-SUB) is limited to version 7.0 or higher.

**1.2. Warranties.** In addition to the warranties and disclaimers set forth in the Master Agreement, Cisco warrants that it will provide the Cloud Services in a manner consistent with general industry standards reasonably applicable to the provision thereof. CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL GUARANTEE ABSOLUTE SECURITYDUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR

INTRUDING UPON AND ATTACKING FILES, NETWORKS AND ENDPOINTS. CISCO DOES NOT REPRESENT OR WARRANT THAT THE CLOUD SERVICES WILL PROTECT ALL END USER FILES, NETWORK, OR ENDPOINTS FROM ALL MALWARE, VIRUSES OR THIRD-PARTY MALICIOUS ATTACKS. CISCO DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES REGARDING ANY THIRD-PARTY SYSTEM OR SERVICE WITH WHICH A CLOUD SERVICE INTEGRATES OR TO ANY ONGOING INTEGRATION SUPPORT. INTEGRATIONS MADE ACCESSIBLE TO SERVICE PROVIDER AND/OR END USER THAT ARE NOT A GENERALLY AVAILABLE PRODUCT INCLUDED ON SERVICE PROVIDER'S AND/OR END USER'S ORDER ARE PROVIDED ON AN "AS IS" BASIS.

**1.3. Privacy Data Sheets for Cloud Services.** For information regarding the processing of personal data by SecureX and Malware Defense (formerly AMP Ecosystem), please see their respective Privacy Data Sheets available on the Cisco Trust Portal.

## 2. Definitions

**2.1. "Endpoint(s)"** means any device capable of processing data and that can access a network, including but not limited to personal computers, mobile devices, and network computer workstations.

**2.2. "Feedback"** means any suggested changes, clarifications, additions, modifications, or recommended product improvements to the MSLA Software that Service Provider or its End Users provide to Cisco as part of technical support or otherwise whether by direct entry into a product user interface, phone conversation, e-mail or otherwise.

**2.3. "Files"** mean those types of files identified in the applicable Documentation, such as an executable, Portable Document Format (PDF), Microsoft Office Documents (MS Word, MS Excel, MS PowerPoint), and those files in a ZIP file (.ZIP).