Service Description: Advanced Services – Fixed Price

Cisco Firepower Solutions Security Deployment Service (ASF-CORE-FW-DEP-IT)

This document describes the fixed price Cisco Firepower Solutions Security Deployment Service. This service covers a variety of Firepower managed device technologies.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/ : (1) Glossary of Terms; (2) List of Services Not Covered. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement"). If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at http://www.cisco.com/web/about/doing_business/legal/terms_conditions.html. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at: http://www.cisco.com/web/about/doing_business/legal/terms_conditions.html. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Cisco Firepower Solutions Security Deployment Service

Service Summary

The Cisco Firepower Solutions Security Deployment Service provides pre-deployment, deployment, and post-deployment activities.

This Service covers the following managed devices and Firepower Solution components:

- One (1) standalone or one (1) High-Availability pair management solution from the following options:
  - FireSIGHT Management Center (FMC)
  - Firepower Management Center (FMC)
- Up to ten (10) total managed devices from the device platform types listed below, of which four (4) may be Firepower Threat Defense or ASA instances on Firepower Security Appliance platforms:
  - FirePOWER Appliances
  - Virtual FirePOWER Appliances
  - FirePOWER Modules (ASA or ISR)
  - Firepower Threat Defense (FTD) on ASA Appliances
  - Virtual Firepower Threat Defense or Virtual NGIPS

Deployment Limitations and Exclusions:

- ISR specific configuration is limited to ISR bootstrapping for FirePOWER module use
- VPN configurations are excluded
- ASA and Firepower clustering is excluded
- Migrations and upgrades are excluded
- Up to fifty (50) unique access control policy rules
- Up to five (5) NAT rules
- Custom signature creation is excluded

This fixed scope service does not cover technology upgrades or migrations from other technologies to Firepower Solution technologies. This fixed scope service does not include configuration of external devices or systems.

Location of Services

Services are delivered both remotely or on-site to Customer as agreed upon. Where Customer desires on-site delivery, travel will be limited to no more than one (1) visit of up to two (2)

days on-site at a single Customer location within EMEAR and APJC regions during Normal Business Hours excluding Cisco holidays and locally recognized country holidays. Where on-site travel is agreed upon, travel must be arranged at least two (2) weeks in advance.

Pre-Deployment

Cisco Responsibilities

- Conduct remote Kick-off call to review project plan and identify key stakeholders from Cisco and Customer. Cisco will provide a timeline/schedule of activities.
- Review the policies for the security solution provided by the Customer.
- Conduct bi-directional knowledge transfer sessions and completion of a Deployment Profile Questionnaire providing a summary of configurations to be implemented.
- Provide remote guidance on rack, stack, and addressing of in-scope Firepower Solution equipment as requested by Customer.

Customer Responsibilities

- Participate in kick-off call and provide Cisco with:
  - Contact information for key stakeholders
  - Policies to be enforced by the security solution
- Provide topology maps, configuration information and existing and proposed Security infrastructure. Customer shall respond to Cisco's requests within two (2) business days for documentation or information required for the service.
- Customer is responsible for rack, stack, and addressing of in-scope Firepower Solution equipment and verifying power, cabling, and IP reachability between FMC(s) and all in-scope Firepower managed devices.
- Providing reasonable remote access to Customer environment to enable service delivery.
- Review with Cisco, and provide answers to, the Deployment Profile Questionnaire.

Deployment

Cisco Responsibilities

- Configure the target Firepower Solution components on the Customer premises (or remotely, as requested by Customer) per the Deployment Profile Questionnaire, subject to travel limitations specified in this Service Description.
- Test the system to ensure proper alerting, dropping, and other pre-defined objectives provided by the Customer and documented in the Deployment Profile Report are met.
- Provide an initial optimization tune based on test results.

Customer Responsibilities

- Participate in scheduled working sessions facilitating Customer side activities to enable Cisco to meet Cisco Responsibilities.

Post-Deployment

Cisco Responsibilities

- Provide a remote supplemental optimization tune approximately 30 calendar days post deployment to improve the security solution in accordance with Customer's goals. Tuning activities may include limiting system "noise," improving alerting, and reducing overall risk to the network.
- Provide Deployment Summary Report.

General Customer Responsibilities

- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Customer will identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers, and project managers.
- Customer will ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Customer will ensure reasonable access to Customer site(s) and facilities including, where applicable, computer equipment, telecom equipment, facilities and workspace. Customer shall provide proper letters of invitation, security clearances and/or escorts as required to access necessary equipment and lab facilities.
- Customer will provide forty-eight (48) hour notice in the event of cancellation of a pre-scheduled meeting.
- Customer expressly understands and agrees that support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer must provide the resources and personnel described in the Customer Responsibilities sections herein to enable Cisco to complete the Services within (90) calendar days after Cisco receives the Purchase Order for the Services.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.