Service Description

Cisco Secure Firewall Implementation Service

(ASF-CORE-FW-DEP)

This Service Description is part of the Services Agreement (as defined in the Services Guide) and describes various Services that Cisco will provide to You. Capitalized terms, unless defined in this document, have the meaning in the Services Guide.

1. Summary

Cisco Secure Firewall Implementation Service provides firewall implementation services ("Services") to Customers for up to one standalone or active/standby high-availability firewall deployment, applying to one of the following products identified at the time of purchase of the Services:

- Cisco Secure Firewall Series 1K
- Cisco Secure Firewall Series 2K
- Cisco Secure Firewall Series 3K
- Cisco Secure Firewall Series 4K
- Secure Firewall Threat Defense Virtual

Location of Services:

- Services will be provided remotely.

Invoicing:

- Services will be invoiced upon completion of the Services.

If a Service or a specific Document Deliverable is listed for review, approval and signoff, the parties will use the Completion and Acknowledgement process documented in the Services Guide.

2. Cisco Responsibilities

- Schedule a one (1) day requirements and design workshop to review design components and use cases.
- Review design components of the environment in comparison to Customer requirements including feature usage, use cases (up to 5), and configuration.
- Analyze existing firewall configurations against Cisco Secure Firewall standard practices.
- Cisco will perform the addition of the devices and the migration on the management platform as well as adding configurations to support the devices.
- Work with Customer to determine test cases relevant to defined use cases.
- Work with Customer to test in accordance with the defined test cases in a lab, as determined by Cisco.

This may be Customer's lab if Customer provides a properly configured lab with the proper equipment.

- Cisco will attend up to 2 change windows up to 6 hours each.
- Conduct a Knowledge Transfer session.
- Provide the following Document Deliverables to the Customer:
  - Solution Design Document (SDD) documenting the requirements, configuration analysis, use cases, migration steps, and proposed high level design of the implementation, provided after the workshop and updated after lab testing.
- Deployment Summary Report (DSR) including test cases, provided after the deployment is completed.
  - Knowledge Transfer (KT) materials, provided at the end of the delivery.

Services are limited by the following assumptions:

- Migration and implementation will be limited to one logical firewall or firewall instance to an FTD logical device.
- Standard practices application will be based on Cisco tools that identify and address standard practice variations.
- For third-party to Cisco migrations, standard practice application will happen post-migration.
- Each context of a multiple context firewall counts as an individual firewall/firewall pair.
- Customer must install the management platform (FMC or cdFMC) and prepare it to manage any new devices prior to Cisco beginning the Services.
- The following are out of scope:
- Multiple instances, multiple contexts, multiple tenants, and similar configurations
- Clustered firewalls are not supported
- Production changes to devices or third party configurations to any devices or platforms other than the management platform and the devices listed in the Summary above.
- Any application configuration, support, or testing.

3. Customer Responsibilities

- Provide Customer design and operational documentation and information including detailed description of Customer's firewall architecture, goals, and requirements.
  - Attend any workshops, or project calls agreed upon and scheduled by the Cisco project manager.
- Racking, stacking, powering, provisioning, and addressing of any equipment or platforms.
- Provide data associated with chassis configurations to provide necessary support during the migration process.