Cisco Secure Remote Worker VPN Implementation Service – Medium (ASF-CORE-SRW-VPN-M) Service Description

General Terms

This document must be read in conjunction with the How Cisco Provides Services document, which is incorporated into this document by reference.

Service Summary: Cisco Secure Remote Worker VPN (Virtual Private Network) Capacity Design and Implementation Service-Medium provides design, configuration, and implementation support to help increase the capacity of your Remote Access VPN.

Table of Contents

1. Service Scope

- Review of Customer's solution requirements, VPN configuration, security policies, hardware capacity, licensing, throughput, and bandwidth.
- Review Customer provided technical documentation and existing design to determine if it meets Customer's business objectives and technical requirements.
- Configure up to two (2) VPN Cluster with up to three (3) Cisco ASA (Adaptive Security Appliances) or up to two (2) FTD (Firepower Threat Defense) with basic configuration for up to five (5) group policies (IP addressing, routing, high-availability for new deployments only) for VPN connectivity.
- Provide As-Built document, which may include the following:
  - Customer's business, technical, and operational requirements.
  - Customer's future business, technical, and operational requirements.
  - Identified feature or functionality gaps.
- Implement VPN-related capabilities in Cisco firewalls.
- Integrate with one (1) existing authentication system.
- Review and validate Customer provided MOP (Method of Procedure) documentation
- Provide Customer with post implementation support covering eight (8) hours over a period of five (5) consecutive business days

2. Out of Scope

- Any migrations from ASA (Adaptive Security Appliance) version 8.x to newer version of ASA or ASA to FTD (Firepower Threat Defense)
- Implementation of ASA software version 8.X or earlier
- Dynamic Access Policies or host scan configuration
- Firewall rule optimization, PKI (Public Key Infrastructure) build-up, IPS/IDS (Intrusion Prevention System / Intrusion Detection System) and host checking
- ISE (Identity Services Engine) device administration, posture, profiling, security group tagging/access, and guest access
- Proactive software recommendations (bug scrub)
- Cisco AnyConnect upgrade, implementation, and migration
- Racking, stacking, powering, base configuration.
- Third party integration (except for 1 authentication system)
- Endpoint configuration and troubleshooting
- Network infrastructure configuration and troubleshooting
- Integration with any SIEM (Security Information and Event Management) systems

3. Service Deliverables

- As-Built Document
- Knowledge transfer materials

4. Location of Service

- Services are delivered remotely to Customer