# Service Description: Advanced Services – Fixed Price

# Network Device Security Assessment (ASF-CORE-SEC-NDSA)

This document describes Advanced Services Fixed Price: Network Device Security Assessment (NDSA).

**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/legal/advancedservices.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/legal/advancedservices.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/.

## Network Device Security Assessment

### Service Summary

The Cisco Network Device Security Assessment Service assesses the security hardening of Cisco devices relative to Cisco security best practices to identify gaps, prioritize and recommend remediation for these gaps ("Services").

The Services provide an assessment for up to five-hundred (500) Cisco network security devices for the following types of platforms:

- Cisco Routers and Switches running IOS, IOSXR, Nexus and CatOS Operating Systems
- Cisco Firewall and VPN devices – ASA, FWSM, ASASM, PIX
- Cisco Intrusion Detection Devices – IPS Sensors and Catalyst 6500 IDS Module

**Location of Services**

Services are delivered remotely to Customer.

**Network Device Security Assessment**

### Cisco Responsibilities

- Review of Customer's network device security goals and requirements.
- Provide the NDSA questionnaire to Customer for completion by Customer; collect the Customer-completed NDSA questionnaire.
- Review the Customer-provided information in response to the NDSA questionnaire, including network device configurations and "show version" and "show running" information.
- Apply Cisco security best practice rules and engineering knowledge to analyze network device configurations and identify gaps in the device security hardening.
- Provide a network device security assessment and document the assessment in a report to include the following information:
  - network security device analysis comparing Customer's current practices to Cisco's recommended best practices;
  - prioritized list of any discovered gaps and critical findings;
  - recommendations for the devices included in the assessment up to five-hundred (500) devices.
- Provide the Network Device Security Assessment Report to Customer.

### Customer Responsibilities

- Provide network device security goals and requirements.
- Complete the NDSA questionnaire, providing information for network security device configurations and "show version" and "show running" information.
- Review with Cisco the information provided by Customer in response to the NDSA questionnaire.

## 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.
- 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.
- 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.
- Support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein.

## 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.