Service Description: Advanced Services – Fixed Price

Cisco Assessment Service for Network Health Check (ASF-SP1-G-NGN-NHC)

This document describes the Advanced Services Fixed Price: Cisco Assessment Service for Network Health Check.

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 Assessment Service for Network Health Check

Service Summary

Cisco shall provide Cisco Assessment Service for Network Health Check to Customer for a health assessment of the Customer's network, including recommendations to promote improvements in overall network health and performance. The Services are comprised of a health index, what-if analysis, and critical health recommendations; and the Services are based on a hardware and software inventory audit, field notices, end-of-life notices, configuration best practices analysis and security advisory analysis.

Location of Services

Services are delivered remotely to Customer.

Cisco Responsibilities

- Conduct network data collection remotely using a Data Collection Tool (DCT); DCT software will be hosted in a Cisco data center, requiring a virtual connection to the Customer's network ("Network") and access to network equipment during the duration of the Services;
- Work with Customer remotely to monitor the progress of CNC data collection; data collection may take up to five (5) days.
- Analyze the collected network data to be used as input for conducting the network health assessment.
- Provide an assessment of the Network, comprised of network health index, what-if analysis and critical health recommendations based on hardware and software inventory audit, applicable field notices, end-of-life, configuration best practices and security advisory analysis for selected product platforms; the total number of devices for data collection shall not exceed five hundred (500) devices.
- Conduct a remote review session with Customer to review the Network Health Assessment and Recommendations for comments and approval.
- Ensure all data and information collected will be protected and made available only to authorized Cisco personnel, used for the sole purpose of the network health assessment.

Customer Responsibilities

- Allow for virtual private network (VPN) access of Cisco software to the relevant areas of the Network for data collection from network devices.
- Obtain for Cisco the required internal security approval related to the data collection and provide relevant permission for virtualized data collection software (DCT) on the Network.
- Notify Cisco about changes made to the Network such as Product(s) added/deleted and changes made to Product credentials.
- Provide resolution of any access problems (Access Control List's, firewall, etc) that may occur between the DCT and the Product(s) in the Network.
- Provide resolution of any data communication problems that may prevent the DCT from uploading data to Cisco or preventing remote maintenance of the DCT.
- Provide to Cisco data communication access to enable VPN client setup.
- Provide Cisco with access to all network devices required for data collection in accordance with the following device preparation:
  - Confirm all Cisco chassis within the target network(s) have the following:
    - IP enabled for every device;
    - SNMP enabled every device;
    - Confirmation of working SNMP Read Only Community String for every device;
    - Telnet or SSH Enabled on every device;
    - Confirmation of at least one of the following three (3) depending upon each device type:
      1) Known, operational Telnet privileged mode 15 password;
      2) Known, operational SSH privileged mode 15 username and password;
      3) Known, operational centralized TACACS. Server username and password up to mode *15*
    - Confirmation that UDP Port 161 SNMP GET data is transmit/receive permitted by the device;
    - Confirmation that TCP Port 23 data is transmit/receive permitted by the device if the device supports Telnet CLI Login authentication;
    - Confirmation that TCP Port 22 data is transmit/receive permitted by the device if the device requires SSH CLI Login authentication;
    - UDP Ports 53, 161, and TCP Ports 22, 23, 53, 80 from the public internet via the Cisco VPN Client;
    - Disable ACL or any firewalls which would prevent SNMP access or CLI access to the devices;
    - Make available UDP port 161 to enable management of devices;
    - For data accuracy reasons, provide TCP port 22 or 23 for Cisco to obtain devices show commands;
    - Provide access to UDP port 53 and TCP port 53 for reporting purposes. If Customer maintains DNS, reporting can be performed via hostnames versus IP addresses.
    - Enable level privilege to issue show running commands to generate Best Practice reports.
  - Cisco System VPN Client Setup requirements:
    - Confirm that IPSec or SSL based Cisco Virtual Private Networking (VPN) network solution is operational, capable of supporting:
      - Minimum 200 kbps streaming bidirectional IP traffic (preferred 1 mbps)
      - Credential information (VPN Server Host/IP Address, VPN Username, VPN Password) supporting access to all Operational IP Networks for ICMP, UDP Ports 53, 161, and TCP Ports 22, 23, 53, 80 from the Public Internet via the Cisco VPN Client.
      - Remove all VPN timeouts or provide VPN timeout rules to Cisco.
      - VPN concentrator should place CNC in a subnet which will have access to all devices.
    - Seed file requirements:
      - Device names or IP addresses;
      - SNMP R/O for all devices;
      - Telnet or SSH credentials for CLI access, and enable password with privilege level 15.
  - Participate in a remote session to review with Cisco the Network Health Report and Recommendations, providing comments and approval.

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.
- Provide a primary point of contact for all initiatives and issues relating to the network health assessment.
- Designate a back up contact when the primary contact is not available.
- 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.