



Service Description: Cisco Security Optimization Service

This document describes Cisco Security Optimization Service.

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; and (3) Severity and Escalation Guidelines. 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, this document is incorporated into your Master Services Agreement (MSA) with Cisco. In the event of a conflict between this Service Description and your MSA, 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/

Service Summary

The Cisco Security Optimization Service is intended to supplement a current support agreement for Cisco products. Cisco shall provide the Security Optimization Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("Quote") setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed upon between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Cisco Security Optimization Service

Cisco Responsibilities:

Cisco shall provide the following during Standard Business Hours (unless otherwise stated):

Security Technology Planning Support. Cisco shall:

- Participate in two (2) strategic planning meetings per year.
- Develop a Security Technology Planning Meeting Report, providing a synopsis of the meeting and documenting significant recommendations. Two (2) reports delivered per year.

- Provide collateral / technical reference material (white papers, technical specifications) as requested for specific technologies or for security architectural approaches.
- Participate in two (2) security technology migration planning sessions.

- **Security Technology Readiness Assessment**

Cisco technical security engineers analyze deployment requirements for a new security solution and assess the readiness of your network devices, operations, security policies, and architecture to support the solution. As part of this service Cisco shall:

- Conduct one (1) design workshop to gather business, technical, and operational requirements including current network design documents and future security technology plans to support the readiness assessment
- Develop one (1) Security Readiness Assessment Report to document findings and recommendations including recommendations for modifications to the network infrastructure and to the parameters for application performance and availability.

- **Internal Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the internal network infrastructure including WANs and LANs for core, campus and individual sites as specified in the Quote. The assessment also covers common security infrastructure controls that apply to many infrastructure domains such as access control, identity management, network management, intrusion detection and prevention, security event management and logging. Based on the scope of the assessment, specific information collected during the Internal SAA may include:

- Network architecture description
- Standards for network infrastructure
- Applications and services running over the network (VoIP, video streaming, terminal emulation, http, ftp, etc.)
- Key network assets, applications and services
- Physical and logical network topology diagrams, including the location of the devices included in assessment

- High-level architecture of data center, internal servers, user host connectivity and Internet connectivity

- Network Management System architecture

- **Perimeter Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the security infrastructure that protects the Customer's network perimeter including internet access, employee remote access, extranet, guest networks, and e-commerce sites as specified in the Quote. Based on the scope of the assessment, specific information collected during the Perimeter SAA may include:

- Network architecture description
- Standards for network infrastructure
- High-level architecture of network perimeter
- Services that traverse the perimeter network
- Key perimeter network assets, application and services
- Physical and logical perimeter network topology diagrams, including the location of the devices included in assessment
- Network Management System architecture
- Access point and controller configurations and templates

Security Design Support. Cisco will conduct an in-depth analysis of the security design to determine its effectiveness for meeting your security business and IT strategies. As part of this design support, Cisco shall:

- Conduct a design workshop to gather data and initiate the development of the security design.
- Analyze network security design against organizational security strategy and requirements.
- Draft recommendations to improving the strength and security of the given design

- **Perimeter Security Posture Assessment ("SPA")**

Cisco will provide a Perimeter SPA designed to assess vulnerabilities in the Customer's Internet-facing IP infrastructure and the effectiveness of email and browser security controls. Due to the global nature of the Cisco Advanced Services team that performs this testing; the Perimeter SPA may be performed at times outside of Standard Business Hours. The following activities will be conducted as part of the Perimeter SPA:

- **Discovery and Vulnerability Identification:** Cisco NCEs will identify and perform a vulnerability assessment and penetration test on IP addresses, not

to exceed the amount specified in the Quote from Cisco, in the Customer's Internet-facing infrastructure from a list that the Customer provides. Specific activities performed during the discovery and vulnerability identification phase include:

- Research and confirm IP and DNS registration of the targeted IP space
- Identify active (live) IP addresses in the targeted Internet-facing infrastructure using ICMP ping and TCP SYN scanning among other techniques as needed
- Scan all 65,535 potential TCP ports and a subset of potential UDP ports on the targeted live IP addresses to identify open ports and services
- **Vulnerability Confirmation and Target Analysis:** Cisco NCEs will attempt to confirm the existence of potential security vulnerabilities identified during the previous activity using a variety of techniques up to and including system-level and secondary exploitation. This activity is designed to provide insight into the potential for successful attacks on the Customer's Internet-facing infrastructure by malicious individuals and the likelihood that the Customer's security and systems administrators would detect these attacks. Specific activities performed during the vulnerability confirmation and target analysis phase include:
 - Confirm vulnerabilities identified during the previous phase using validated and tested exploits and penetration testing techniques
 - Analyze the risk posed by exploitable vulnerabilities to the Customer's environment via secondary exploitation and data mining of compromised systems vulnerabilities; and recommendations for improvement

Security Change Support.

- Cisco will provide designated engineer ("Advanced Service Engineer") when Customer is making changes it deems critical to the Network's advanced security technologies (CSA, MARS, CSM, and IPS).
 - Scheduled Change. Cisco will make available, upon receipt of not less than twenty-one (21) days prior written request by Customer to Cisco, a designated support contact that can consult with Customer on a 24-hour 7-day standby basis to provide remote engineering support during scheduled change window, not to exceed one (1) per quarter.
 - Unscheduled Change Support. Cisco will provide remote engineering support to provide support during an unscheduled change window, not to exceed one (1) per quarter, to Network to Customer to minimize the impact of individual device failures on the overall Network. Customer must open a service request with

the Cisco's TAC prior to contacting Advanced Service Engineer for any unscheduled change support. To support any unscheduled changes to Network, Cisco will:

- Designate an engineer ("Advanced Services Engineer") to act as the primary technical contact to with Customer and Cisco Technical Assistance Center (TAC).
- Provide technical evaluation of initial TAC problem diagnosis based on knowledge of Customer's Network.
- Provide technical evaluation of proposed unscheduled change to Network.
- Provide technical representation in regularly scheduled conference calls.

Knowledge Transfer and Mentoring.

- Conduct an evaluation working session (1) to gather Customer's requirements for knowledge transfer to support design and configuration tasks.
- Provide a summary report of knowledge transfer requirements coming from the workshop including a proposed twelve (12) month schedule of knowledge transfer activities.
- Provide four (4) quarterly onsite chalk talks and technical presentations on advanced security technologies during quarterly review visits as requested.
- Provide informal mentoring during security technology design and configuration tasks.
- Provide two (2) – three (3) hour knowledge transfer sessions delivered remotely. Sessions support up to twenty-five (25) students.

Customer Responsibilities

• General Responsibilities

- Designate at least two (2) but not more than six (6) technical representatives, who must be Customer's employees in a centralized Network support center (Customer's technical assistance center), to act as the primary technical interface to the Advanced Services Engineer. Customer will designate as contacts senior engineers with the authority to make any necessary changes to the Network configuration. One individual, who is a senior member of management or technical staff, will be designated as Customer's primary point of contact to manage the implementation of services under this Exhibit (e.g., chair the weekly

conference calls, assist with prioritization of projects and activities).

- Within one (1) year from the commencement of this Exhibit, Customer will have at least one (1) Cisco Certified Internetworking Expert ("CCIE") trained employee or one (1) employee that have achieved, in Cisco's sole determination, an equal standard through training and experience as designated contacts.
- Customer's technical assistance center shall maintain centralized network management for its Network supported under this Exhibit, capable of providing Level 1 and Level 2 support.
- Provide reasonable electronic access to Customer's Network to allow the Advanced Services Engineer to provide support.
- If Cisco provides Data Collection Tools or scripts located at Customer's site, Customer shall ensure that such Data Collection Tools or scripts are located in a secure area, within a Network environment protected within a firewall and on a secure LAN, under lock and key and with access restricted to those Customer employee(s) or contractor(s) who have a need to access the Data Collection Tools and/or a need to know the contents of the output of Data Collection Tools. In the event Data Collection Tool provided by Cisco is Software, Customer agrees to make appropriate computers available and download Software as needed. Customer shall remain responsible for any damage to or loss or theft of the Data Collection Tools while in Customer's custody.
- Provide a Network topology map, configuration information, and information of new features being implemented as needed.
- Notify Advanced Services Engineer of any major Network changes (e.g., topology, configuration, new IOS releases.).
- In the event the Network composition is altered, after this Exhibit is in effect, Customer is responsible to notify Cisco in writing within ten days (10) of the change. Cisco may require modifications to the fee if the Network composition has increased beyond the original pricing quote for Services.
- Create and manage an internal email alias for communication with Advances Services Engineer.
- Retain overall responsibility for any business process impact and any process change implementations.

- **Security Technology Planning Support.** In addition to the General Responsibilities, Customer shall provide the following:
 - Establish and inform Cisco of dates at least sixty (60) days in advance strategic planning meetings per year.
 - Develop a Security Technology Planning Meeting Report, providing a synopsis of the meeting and documenting significant recommendations. Two (2) reports delivered per year.
 - Provide collateral / technical reference material (white papers, technical specifications) as requested for specific technologies or for security architectural approaches.
 - Participate in two (2) security technology migration planning sessions.
- **Security Technology Readiness Assessment.** In addition to the General Responsibilities, Customer shall provide the following:
 - Designate a program manager to act as the single point of contact to which all Cisco communications may be addressed, having an appropriate level of Network experience. Such person shall act as Customer's host for onsite assessment activity to coordinate facility access, conference rooms, phone access and staff scheduling.
 - Ensure key engineering, networking and operational personnel are available to participate in interview sessions as required by Cisco in support of an assessment. Review assessment report and suggestions provided by Cisco.
 - Assessment data collection support.
 - Customer agrees to make its production, and if applicable, test Network environment available for installation of Data Collection Tools. Customer shall ensure that Cisco has all relevant Product information needed for an assessment.
 - Customer shall advise Cisco immediately of all adds, moves and changes of the Product within Customer's Network.
 - Assemble all necessary Network availability data to enable Cisco to calculate quarterly Network availability. The type of data required to perform the calculations includes the following:
 - Outage Start Time (date/time)
 - Service Restore Time (date/time)
 - Problem Description
 - Root Cause
 - Resolution
 - Number of end users impacted
 - Equipment Model
 - Component/Part
 - Planned maintenance activity/unplanned activity
 - Total end user/ports on network
- **Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall provide the following:
 - Assessment data collection support.
 - Provide a list of all of the existing security architecture components including but not limited to Hardware, Software and solution configurations; architecture descriptions.
 - Provide a high-level architectural drawing showing the type of Hardware, Software, and application solutions configurations and where they are physically located (for example, geographical location or location within the Network).
 - Provide detailed definitions of the type of application (for example mobile traveler, corporate workforce) and features; detailed definition of Customer's implementation strategy.
 - Provide copies of product configuration templates.
 - Provide security network expansion roadmap.
 - Provide a network topology map, configuration information, and information of new features being implemented as needed.
 - Retain overall responsibility for any business process impact and any process change implementations.
 - Ensure key Customer networking and operational personnel are available to participate in interview sessions as required.
 - Unless otherwise agreed to by the parties, Customer shall respond within two (2) business days of Cisco's request for documentation or information needed for the Service.
 - Customer acknowledges that Cisco's obligation is to only provide assistance to Customer with respect to the tasks detailed and that such assistance may not result in some or all of the tasks being completed.

- **Design Support.** In addition to the General Responsibilities, Customer shall provide the following:
 - Provide the low level design document describing how the Customer Network needs to be built and engineered to meet a specific set of technical requirements and design goals. The level of details must be sufficient to be used as input to an implementation plan.
 - Ensure key detailed design stakeholders and decision-makers are available to participate during the course of the Service.
 - Provide or extract additional information required in the design effort (e.g., current and planned traffic characteristics).
 - Any documentation of business requirements and technical requirements for the new design.
 - Any Information on Information on current and planned traffic characteristics or constraints.
- **Perimeter Security Posture Assessment (“SPA”).** In addition to the General Responsibilities, Customer shall provide the following:
 - Information about IP addresses to be included in perimeter penetration testing.
 - Data collection activities as needed to facilitate a specific Cisco analyses.
- **Network Change Support.** In addition to the General Responsibilities, Customer shall provide the following:
 - Designate person(s) from within its technical support organization to serve as a liaison to the Advanced Services Engineer.
 - Provide its designated person(s) with instructions on process and procedure to engage the Advanced Services Engineer.
 - Information on architecture (which may include remote sites and size of remote sites).
 - Identify low risk and high risk areas of the Network based on their Network traffic.
 - Information on Customer Implementation plan and deployment schedule.
 - Maintenance window information and any other constraints.
 - Information on Customer change control process.
- Contact information and customer escalation process.
- Review details of planned changes with Advanced Services Engineer.
- Advise Cisco of its standard operating procedures related to its business practices, its internal operational nomenclature and Network to allow Cisco to effectively communicate and discuss changes with Customer in the context of Customer’s business environment.
- Provide all necessary information to enable Cisco to perform root cause analysis.
- Provide reasonable electronic access to Customer's Network to assist Cisco in providing support.
- **Knowledge Transfer and Mentoring.** In addition to the General Responsibilities, Customer shall provide:
 - Details on desired topics Customer wants to see covered through knowledge transfer and mentoring, with background information on the skill sets of the audience or mentoring program participants.
 - Ensure that facilities and equipment are available to host the informal technical update sessions.