Service Description: Cisco Service Provider Security Optimization Service

This document describes the Cisco Service Provider 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/

The Cisco Service Provider 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. Availability of services described herein and delivery may vary by geographical region.

Service Summary

The Cisco Service Provider Security Optimization Service provides Annual Assessments, Network Support and Continuous Learning service modules.

Services provided under this Service Description will build upon Cisco's Service Provider Foundation Technology Optimization Service.

General Service Responsibilities of Cisco

Cisco's Service Provider Security Optimization Service consists of, at a minimum, Design Support from the list described below.

Cisco shall support the following General Service provisions for any Service Provider Security Optimization Service specified in the Quote:

- Designate an engineer ("Network Consulting Engineer") to act as the primary interface with the Cisco project manager appointed for the Customer
- Participate in regular visits to the Customer as required by the project manager either via phone or in-person to review proactive deliverables and activities and to plan for next quarter. In-person visits not to exceed eight (8) days in aggregate. Additional visits will be mutually agreed at Cisco's then-current travel and labor rates
- Designate engineer(s) to work with the Cisco project manager and the primary Network Consulting Engineer
- Participate in periodic conference calls (usually weekly) to review Customer's Network status, planning and the Services being provided
- Monitor a Customer-specific Cisco email alias to facilitate communication with primary Network Consulting Engineer as well as the engineers on Cisco's SP Security team
- Network Consulting Engineer may utilize Customer provided data, scripts or internal tools to assist in collecting data from the Network.

Specific Service Responsibilities of Cisco

In addition to the General Responsibilities, Cisco shall provide the following:

Annual Assessments

Network Device Security Assessment (NDSA)

Cisco will consult with Customer via a series of meetings to understand and analyze aspects of Customer's Network device security. A Network Device Security Assessment will be performed on up to 350 security devices and may include, among other information, the following:

- Review of Customer's Network device security goals and requirements;
- Analysis of network device configurations focused on security hardening of the individual devices;
- Analysis of firewall rules for common configuration issues;
- Report describing the analysis comparing Customer's current practices to Cisco's recommended best practices and Cisco's recommendations (sampled based on size and configuration of network);
- Report describing prioritized list of discovered vulnerabilities and most critical findings; and,
- Interactive presentation of findings, analysis, and recommendations.

Network Security Architecture Assessment ("SAA")

Cisco's Network Consulting Engineer assesses the effectiveness of the Cisco Security Control Framework/Technical Control Set in the network infrastructure.

- Scope and Collect:
  - Conduct discussions, interviews and whiteboard sessions with the Customer's representatives to gather general information about Customer's: business and network architecture, compliance requirements, future business plans that affect the network infrastructure, Security organization, strategy and policies, Security concerns and previous incidents
  - Identify specific network assets to include in assessment, not to exceed the amount specified in the Quote from Cisco
  - Collect detailed information: network topology, architecture and design documents, device configurations for core, distribution, access and edge devices, configuration templates
  - Refine collected information remotely through e-mail and phone conversations with Customer's representatives
- Assess:
  - Identify architectural techniques used to implement security controls
  - Assess effectiveness of techniques
  - Evaluate how widely techniques are deployed
- Report:
  - Identify gaps in controls based on lack of architectural support for the control or incomplete deployment of control
  - Evaluation of gaps relative to business objectives
  - Remediation recommendations for the highest level risks
- Present:
  - Conduct a final Workshop to present findings, analysis and recommendations
  - Run a question & answer (Q&A) session

Security Posture Assessment

Cisco's Network Consulting Engineer assesses vulnerabilities in the Customer's IP network both from an Inter- and Intra-Autonomous System standpoint. Assessment activities will be performed remotely and possibly outside of Standard Business Hours.

- Discovery and Vulnerability Identification:
  - Identify live IP addresses, not to exceed the number specified in the Quote from Cisco, within the Customer's Autonomous System and outside of the Customer's Autonomous System from a list of IP addresses provided by the Customer.
- Vulnerability Confirmation and Target Analysis:
  - Confirm the existence of identified potential security vulnerabilities using a variety of techniques.
- Results Analysis and Presentation:
  - Compile and analyze vulnerabilities, risks and exposure, and provide an executive-level presentation summarizing the assessment findings and results in a prioritized manner along with recommendations to mitigate high-severity findings.

Network Support

New Security Technology Planning Support

Cisco Network Consulting Engineer provides strategic as well as tactical guidance through participation in periodic security technical planning meetings. Meeting topics are aligned to your business goals and objectives and may cover a range of topics from near-term solutions to evolving security threats and longer-term management planning.

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

Develop a New Security Technology Planning Meeting Report, providing a synopsis of the meeting and documenting significant recommendations. Two (2) reports delivered per year.

Security Design Support

Cisco's Network Consulting Engineer conducts an in-depth analysis of the security design to determine its effectiveness for meeting Customer's network security strategies.

Cisco's Network Consulting Engineer also provides ongoing design consultation to the Customer.

As part of this design support, Cisco shall:

- Consult with Customer networking staff in a series of meetings to develop a thorough understanding of Customer Network design requirements, priorities and goals with a focus on concerns such as resiliency, self-recovery, scalability, and ability to handle increased traffic demands and QoS.
- Provide a detailed design report with recommendations that take into consideration, among other things, the following:
  - Customer design requirements, priorities and goals
  - Analysis of impact of new design requirements on existing network
  - Architecture and topology for the network
  - Protocol selection and configuration
  - Feature selection and configuration
  - Customer's network Security design vs. organizational Security strategy and requirements

Security Change Support

Cisco's Network Consulting Engineer provides expertise when making critical changes to the network's advanced security technologies. Change support typically involves reviewing and recommending any needed changes to the design, implementation plan, test plan, and rollback plan for the change, implementation support during the change window, and post implementation support including stabilization, troubleshooting incidents and root cause analysis for unscheduled network outages.

- Cisco will provide designated engineer when Customer is making changes it deems critical to the Network's advanced security technologies (CSA, MARS, CSM, and IPS).
- Designated engineer acts as the primary technical contact to Customer and Cisco Technical Assistance Center (TAC).
  - Scheduled Change Support: Cisco will make available, upon receipt within a mutually agreed time window, a designated support contact that can consult with Customer to provide remote engineering support.
  - Unscheduled Change Support: Cisco will provide remote engineering support to Customer during an unscheduled change window, in order to minimize the impact of individual device failures on the overall Network. To support any unscheduled changes to Network, Cisco will:
    - Provide technical evaluation of initial TAC problem diagnosis based on knowledge of Customer's Network.

<u>Continuous Learning</u>

Security Knowledge Transfer and Mentoring

Cisco's Network Consulting Engineer prepares your staff to effectively operate, maintain, manage, and tune their Cisco Self-defending Network through ongoing knowledge transfer sessions.

- Conduct an evaluation working session 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.

General Service Responsibilities of Customer

Customer shall comply with the following General Service provisions for any Security Optimization Service specified in the Quote:

- 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 Network Consulting 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).
- Ensure key engineering, networking and operational personnel are available to participate in interview sessions and review reports as required by Cisco in support of Service.
- 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 Network Consulting Engineer to provide 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.
- 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 Network Consulting 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.
- Supply the workplace policies, conditions and environment in effect at the Customer's facility.
- Provide proper security clearances and/or escorts as required to access the Customer's facility.
- Customer agrees that it will not hire a current or former employee of Cisco, who is involved in the Services under this Service Description, during the term of the Service and for a period of one (1) year after the termination of the Service. As liquidated damages, and not as a penalty, should Customer hire a current or former Cisco employee who is involved in the Services under this Service Description, Customer shall pay to Cisco three (3) times the annual compensation of such employee on the date the employee is hired. If payment is not made on such date, the liquidated damage payment shall be six (6) times the annual compensation of such employee.

Specific Service Responsibilities of Customer

In addition to the General Responsibilities, Customer shall provide the following:

<u>Annual Assessments</u>

Network Device Security Assessment (NDSA)

- List of up to 350 devices to be included in assessment,
- Supply device configurations and versions, and,
- Supply relevant network topology diagrams.

Security Architecture Assessment

- 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.

Security Posture Assessment

- Information about IP addresses to be included in testing access from within and from outside Customer's Autonomous System.
- Data collection activities as needed to facilitate a specific Cisco analysis.

<u>Network Support</u>

New Security Technology Planning Support

- Establish and inform Cisco of dates at least sixty (60) days in advance strategic planning meetings per year.
- Provide technology roadmaps necessary to support the planning sessions.

Security Design Support

- 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.

Security Change Support

- Designate person(s) from within its technical support organization to serve as a liaison to the Network Consulting Engineer.
- Provide its designated person(s) with instructions on process and procedure to engage the Network Consulting 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 Network Consulting 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.

Continuous Learning

Security Knowledge Transfer and Mentoring

- 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.