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.

General Service Responsibilities

Cisco and the Customer shall have general responsibilities found in this section below.

General Service Responsibilities of Cisco

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

- Under this Service, Cisco shall provide the Security Optimization Service during Standard Business Hours, unless stated otherwise.
- Provide a single point of contact ("Cisco Project Manager") for all issues relating to the Services.
- Participate in regularly scheduled meetings with the Customer to discuss the status of the Services.
- Ensure Cisco employees (including Cisco subcontractors) conform to Customer’s reasonable workplace policies, conditions and safety regulations that are consistent with Cisco’s obligations herein and that are provided to Cisco in writing prior to commencement of the Services; provided, however, that Cisco’s personnel or subcontractors shall not be required to sign individual agreements with Customer or waive any personal rights.
- Supply Cisco project team personnel with a displayable form of identification to be worn at all times during services activities at Customer’s facility.
- Cisco reserves the right to determine which of its personnel shall be assigned to a particular project, to replace or reassign such personnel and/or subcontract to qualified third persons part or all of the performance of any Security Optimization Service hereunder. Should Customer request the removal or reassignment of any Cisco personnel at any time; however Customer shall be responsible for extra costs relating to such removal or reassignment of Cisco personnel. Cisco shall not have any liability for any costs, which may occur due to project delays due to such removal or reassignment of Cisco personnel.

General Responsibilities of Customer

General Services

Customer shall comply with the following obligations for General Services 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 security engineer or administrator role, to act as the primary technical interface to the Cisco designated engineer(s). 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 Service Description (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.
- Customer's technical assistance center shall maintain centralized network and security management for its Network supported under this Service Description, capable of providing Level 1 and Level 2 support.
- Provide reasonable electronic access to Customer's Network to allow the Cisco designated 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.
- Provide requirements documentation, low-level and high- level designs, implementations plans, and test plans as required for specific services.
- Notify Cisco immediately of any major security policy (e.g. firewall rule change; Cisco ISE policy change) or Network changes (e.g. topology; configuration; new IOS releases; moves, adds, changes and deletes of devices).
- In the event the Network or Security composition is altered, after this Service Description 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 Cisco.
- 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.

In addition to the General Responsibilities, Cisco and the Customer each shall comply with obligations as required for specific security services.

Specific Integration Service Details (CON-AS-SEC)

This section provides the service details for the following Integration services:

Network Device Security Assessment (**OPT-SOS-NDSA**)

Specific Service Responsibilities of Cisco

Cisco will consult with the Customer to provide a review of the NDSA service, answer questions, and establish mutually-agreed upon expectations for the scope of the assessment and the level of device configuration sampling. Network Device Security Assessment may include, among other information, the following:

- Assess up to 350 Cisco device configurations, but only 10 of those devices may be firewalls.
- Review of Customer's device security templates.
- Provide an encrypted method for the customer to provide device configurations and policies.
- Analyze device configurations focused on configuration security hardening of the individual devices.
- Analyze firewall rules for common configuration issues.
- Provide secure encrypted delivery of the Assessment Report, which will include: Gap assessment comparing Customer's current practices to Cisco's recommended best practices, and Prioritized list of discovered vulnerabilities and most critical findings.
- An interactive presentation of findings, analysis, and recommendations.
- The deletion, removal, and destruction of collected customer data (device list, device configurations, and device policies) from Cisco repositories.
- The deletion, removal, and destruction of all draft versions of the assessment report.

Specific Service Responsibilities of the Customer

Customer agrees to provide individuals with appropriate expertise and information about the network devices to meet with Cisco to provide information on the Customer desired goals and outcomes of the assessment, and insights into relevant business and technical requirements. Once the specialized assessment team has started analyzing configurations, the device list and configurations may not be changed. Customer is responsible for the following:

- Provide a list of up to 350 devices, of which 10 may be firewalls, to be included in the assessment.
- Supply all listed device configurations and versions in a secure, encrypted manner.
- Ensure all device configurations and versions are accurate and up-to-date.
- Confirm that configurations submitted match the Customer device list.
- Ensure all relevant Customer stakeholders attend the Cisco interactive presentation of findings, analysis, and recommendations.
- Review and submit comments and requests for changes within 10 business-days of the Cisco interactive presentation of findings, analysis, and recommendations.
- Request in writing by an authorized person, the destruction of the finalized assessment from Cisco repositories.

Security Advanced Change Support (**OPT-SOS-ACS**)

Specific Service Responsibilities of Cisco

Security Advanced Change Support consists of a Cisco Security Consulting Engineer to support design of Customer plans (network drawings, implementation plan, test plan rollback plan), and configuration changes (device configurations and cabling changes).

Emergency Changes. Cisco's ability to support an emergency change is dependent on availability of resource. Cisco has no obligation to support an emergency change if Cisco is unable to assign a Cisco Security Consulting Engineer to support the change.

Planned Changes. For planned changes (scheduled twenty-one (21) calendar days in advance), Cisco will have a Cisco Security Consulting Engineer assigned.

During the change window, the Cisco Security Consulting Engineer will observe, provide input and feedback, and will engage directly when authorized. In the case of a rollback, the Cisco Security Consulting Engineer will support de-briefing activities, lessons-learned, and moving forward planning. The Cisco Security Consulting Engineer will support post-change efforts to validate stability and operational functionality. Other Cisco responsibilities include:

- Plan Development and review of existing plans (e.g., network drawings, implementation plan, test plan, rollback plan).
- Review with Customer for input, recommendations and feedback on plans.
- Plan Development and review of planned changes (e.g., device configurations, cabling changes).
- Provide Change Plan and Device Configurations Report.
- Change Support Window (e.g., troubleshooting support, implementation support, support relevant Customer opened TAC cases).
- Post- Change Implementation Support (e.g., troubleshooting support, performance review, stabilization efforts).

Limitations:

- Changes may not include more than two (2) security devices or two (2) pairs of security devices (e.g., active-standby firewall pairs).
- Changes may not include more than ten (10) network devices.
- Cisco will determine the content and format of the deliverable.
- A change support window may not be longer than eight (8) hours. There may be no more than two (2) change support windows. Change support windows may be after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide its designated person(s) with instructions on process and procedure to engage the Cisco designated engineer.
- Provide Schedule, Change Window Information, change control process, escalation process, standard operating procedures, relevant nomenclature, and any other known, relevant constraints.
- Support development and review change plans (e.g., network drawings, implementation plan, test plan, rollback plan) with Cisco designated engineer.
- Provide recommendations and feedback on plans; provide explicit acceptance and rejections of recommendations.
- Support development and review planned changes (e.g., device configurations, cabling changes) with Cisco security engineer.
- Provide recommendations and feedback on planned changes; provide explicit acceptance and rejections of recommendations.
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Customer is responsible for migrating any content to a Customer template or any customizations.
- Customer is responsible for any Customer-specific forms, documents, scheduling responsibilities, Customer internal processes, etc.
- Customer is responsible for opening any cases with vendor's technical assistance center during change window (e.g. Cisco TAC)
- Customer is responsible for making configuration changes to devices.

Security Change Support (**OPT-SOS-CS**)

Specific Service Responsibilities of Cisco

Under Security Change Support (Security CS), Cisco will provide a Cisco designated engineer available during scheduled (planned or emergency) changes to the network, security devices, and security policies for the production environments.

Emergency Changes. Cisco's ability to support an emergency change is dependent on availability of resource. Cisco has no obligation to support an emergency change if Cisco is unable to assign a Cisco designated engineer to support the change.

Planned Changes. For planned changes (scheduled twenty-one (21) calendar days in advance), Cisco will have a Cisco designated engineer assigned.

During the change window, the Cisco designated engineer will observe, as the plan is executed, provide recommendations and feedback as needed, and will engage directly when authorized. In the case of a rollback, the Cisco designated engineer will support de-briefing activities, lessons-learned, and moving forward planning. The Cisco designated engineer will support post-implementation efforts to check the stability and operational functionality. The activities associated with this service should not exceed a period of seven (7) calendar days and will include the following:

- Review of Customer plans (e.g., network drawings, implementation plan, test plan, rollback plan).
- Provide recommendations and feedback on Customer plans.
- Reviewing Customer planned changes (e.g., device configurations, cabling changes).
- Provide recommendations and feedback on Customer planned changes.
- Change Window Support (e.g., troubleshooting support, implementation support, support relevant Customer opened TAC cases).
- Support of Post-Implementation Plan (e.g., troubleshooting support, performance review, stabilization efforts).

Reactive Support: Security Change Support is intended for planned changes. However, Customers may leverage/apply entitlement for this service for reactive situations that are unrelated to planned changes. In these instances, Cisco would provide the following:

- Provide technical evaluation of initial TAC problem diagnosis based on knowledge of Customer's network,
- Provide technical evaluation of proposed unscheduled change to Network, and,
- Provide technical representation in regularly scheduled conference calls.

For reactive situations (e.g., device failure, network outage), Customer may leverage the Security Change Support service for lifeline support; however, the following conditions apply:

- Customer must open a service request with the vendor's technical assistance center (e.g. Cisco TAC) prior to requesting support under Security Change Support.
- Entitlement for 1 unit of change support may not exceed forty (40) hours of support.
- Entitlement for 1 unit of change support may not exceed seven (7) calendar days.
- Root cause analysis is explicitly excluded; the Security Issue Resolution and Planning Support offers support for root cause analysis.

Limitations:

- A change support window may not be longer than eight (8) hours. There may be no more than two (2) change support windows. Change support windows may be after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide its designated person(s) with instructions on process and procedure to engage the Cisco designated engineer.
- Provide Schedule, Change Window Information, change control process, escalation process, standard operating procedures, relevant nomenclature, and any other known, relevant constraints.
- Provide and Review Customer changes plans (e.g., network drawings, implementation plan, test plan, rollback plan) with Cisco security engineer.
- Consider Cisco's recommendations and feedback on Customer plans; provide explicit acceptance and rejections of recommendations.
- Provide Customer planned changes (e.g., device configurations, cabling changes) with Cisco security engineer.
- Consider recommendations and feedback on Customer planned changes; provide explicit acceptance and rejections of recommendations.

- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Making configuration changes to devices.

For **Reactive Support** (e.g., device failure, network outage) unrelated to planned changes, Customers may leverage entitlement for Security Change Support to request assistance. Customer responsibilities in such cases include:

- Opening a service request with the vendor's technical assistance center (e.g. Cisco TAC) prior to requesting entitlement for reactive support.
- Ensure that Cisco security engineer has access to TAC case and notes, if non-Cisco TAC.
- Ensure that Cisco security engineer is included on all calls and discussions with TAC.
- Review with Cisco security engineer any proposed changes.

Security Design Development Support (OPT-SOS-DDS)

Specific Service Responsibilities of Cisco

Cisco responsibilities under Security Design Development Support are limited up to one (1) complex solution set (e.g., Cisco ISE, Cisco Secure ACS, 802.1x deployments) or one (1) non-complex solution set up to forty (40) devices and include the following:

- Provide a Design Development Questionnaire
- Assist with or create Customer Requirements Document, as identified in the Quote
- Review Customer's requirements documentation and re-validate the requirements with Customer.
- Assist with either the High-Level Design Document or the Low-Level Design Document.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide a completed Design Development Questionnaire, which will capture information such as the existing network infrastructure design, existing security infrastructure designs, planned designs, further growth requirements and additional customer requirements.
- Provide either the low-level or high-level design document describing the specific set of technical requirements and design goals and specifying the resulting Customer Network architecture and build-out plans to meet those requirements. The level of details must be sufficient to be used as input to an implementation plan.
- Provide or extract additional information required in the design effort (e.g., current and planned traffic characteristics).
- Provide documentation of any business requirements and technical requirements for the new design.
- Ensure all relevant customer stakeholders attend the Cisco interactive presentation of the Design Document recommendations.
- Review and submit comments and requests for revisions within 10 business-days of the Cisco interactive presentation of the Design Document.

Security Design Review and Support (OPT-SOS-DRS)

Specific Service Responsibilities of Cisco

Cisco will consult with Customer via a series of remote meeting, up to 40 hours of support, to develop a thorough understanding of Customer's security design requirements and will perform the following:

- Review of Customer's design requirements, priorities, and goals.
- Review of security architecture and topology.
- Address design related questions.
- Analysis of impact of new requirements on existing network.
- Review and support of protocol design, selection and configuration.
- Review and support of feature design, selection and configuration.
- Review of device security considerations.
- Informal recommendations or advice about a security design.
- Help Customer resolve minor design-related issues

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide the low level design document describing the specific set of technical requirements and design goals specifying the resulting Customer Network architecture and build-out plans to meet those requirements. 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).

- Provide documentation of any business requirements and technical requirements for the new design.
- Provide information on any current and planned traffic characteristics or constraints.

Security Health Check (**OPT-SOS-HC**)

Specific Service Responsibilities of Cisco

Cisco will perform a Security Health Check, limited to up to one (1) solution set or one (1) complex system (e.g., Cisco ISE, Cisco Secure ACS, 802.1x deployments) and up to twenty (20) devices responsibilities. Responsibilities will include:

- Review Customer's Security Health Check Request Questionnaire.
- Establish health check requirements, strategies, and schedules with Customer.
- Analyze configuration and policy implementations and align them with corporate security policies and procedures, and Cisco best practices,
- Analyze security devices.
- Recommend tuning changes to policy and devices configurations.
- Recommend design or architecture reviews, if needed.
- Identify relevant under-utilized product and solution capabilities.
- Conduct an Informal Knowledge Transfer on identified, relevant under-utilized capabilities (up to 2 hours in duration).
- Perform one (1) interactive tuning session with Customer to implement tuning recommendations.
- Provide a Security Health Check Report

Limitations:

- Performance tuning may be after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Complete the Security Health Check Request Questionnaire.
- Review completed Security Health Check Request Questionnaire with Cisco.
- Establish health check requirements, strategies, and schedule with Cisco.
- Provide electronic access to Cisco to devices such that analysis and tuning may be completed.
- Review and authorize Cisco's recommendations for tuning.
- Change management and scheduling of performance tuning.
- Assisting with interactive tuning session with Cisco to implement tuning recommendations.

Security Issue Resolution and Planning Support (**OPT-SOS-ISUPP**)

Specific Service Responsibilities of Cisco

Cisco will review the security issues, identify the cause, and test and validate to confirm the issues have been identified with a proposed plan to address the issues. Cisco responsibilities include:

- Collect all relevant information regarding the issue.
- Analyze information.
- Review of Customer's device security goals and requirements.
- Provide secure, encrypted method for the Customer to provide device configurations and policies.
- Interactive presentation of findings, analysis, and recommendations.

Limitations:

Given the variety of situations and issues that may be encountered in production environments, issues may require a variety of services to compliment this service. For example:

- Security VTS or Security VTPS may be required to test and confirm causes in a lab environment.
- Design-related issues may require design-related services to produce a viable plan.
- Security IRPS provide insight in causes and a plan for resolving; however, executing the plan may require follow-on services.

Other limitations include:

- There is no guarantee that the root-cause analysis will result in a root-cause being identified or confirmed.
- Reasonable efforts will be made to provide conclusive findings and an issue resolution plan. Regardless, entitlement of an appropriate number of service units will be retired. For example, after a reasonable effort, including a Security VTPS lab re-

create, to deduce the root-cause failure of one (1) security device that results in no-problem found, entitlement to one (1) unit of Security IRPS and one (1) unit of Security VTPS will be retired.

- Cisco Services may have to defer to product development engineering.
- Work may occur after Standard Business Hours.

Each unit of Security IRPS includes:

- Up to one (1) root-cause analysis; although, there may be multiple contributing causes.
- Up to six (6) security and/or network devices.
- Limited up to 80 hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Supply all listed device configurations and versions in a secure, encrypted manner.
- Ensure all device configurations and versions are accurate and up-to-date.
- Ensure all relevant customer stakeholders attend the Cisco interactive presentation of findings, analysis, and recommendations.
- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Open any necessary cases with vendor's technical assistance center (e.g. Cisco TAC).

Security Kick-Start Support (**OPT-SOS-KICK**)

Kick-Start Support is generally initiated following the completion of a Security Health Check where Cisco has identified product or solution capabilities that the Customer may be under-utilizing. Cisco will consult with the Customer to establish a plan and schedule for the Security Remote Knowledge Transfer, Security Design Review and Support, Security Change Support, and Security Performance Tuning further defined in this Service Description.

Security Knowledge Service (**OPT-SOS-KS**)

Specific Service Responsibilities of Cisco

Cisco will provide Security Knowledge Service, through a secure web-based portal ("Portal"). In addition to the security product and technology knowledge services included in this service, the Customer will also be provided with access to the foundational Network Infrastructure Modular Knowledge Service at no additional charge. Cisco responsibilities include:

- Customer user account creation for the Portal.
- Assist with getting the Security Knowledge Service operational with appropriate authentication and authorizations for user community.
- Release security content to the registered number of authorized viewers.
- Security content may be white papers, case studies, design guides, configuration guides, troubleshooting guides, training documents, deployment guides, or online books and/or manuals.
- Archive Customer-specific deliverables when delivered as part of an Advanced Services subscription engagement.
- Update Security content as Cisco may revise, update, and/or remove previously-released multimedia clips and/or content.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) to be responsible for management of portal accounts within user community.
- Provide list of initial set of users to be authorized on the portal.

Security Network Consulting Support (**OPT-SOS-NCS**)

Where available, Cisco will provide Network Consulting Support in the form of a designated engineer ("Advanced Services Engineer") to act as the primary interface with Customer, providing general advice and guidance related to Customer's Network, assessment recommendations, and remediation plans, up to five days per week (pending local work restrictions) during Standard Business Hours excluding Cisco holidays, locally recognized country holidays, vacation, and training days. Customer directed tasks to be performed by the Advanced Services Engineer are subject to Cisco approval, which shall not be unreasonably withheld..

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide Cisco with direction of activities and projects on which the Customer needs the Cisco engineer to engage.

Security Ongoing Flexible Support (OPT-SOS-OFS)

Cisco will provide informal, Ongoing Flexible Support for incremental changes to the network security architecture. This flexible support may be applied to other work items within Security Optimization Service and 1 Unit is limited to 40 hours of assigned engineer's time. Cisco engineers will be assigned as work items are selected throughout the term of the service contract.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide Cisco with details around what type of support is needed when a request is made.

Security Performance Tuning Support (OPT-SOS-PTS)

Specific Service Responsibilities of Cisco

Cisco will provide Security Performance Tuning Support, consisting of the following:

- Meet with Customer to review Security Performance Tuning Support Questionnaire.
- Meet with Customer to establish performance tuning requirements, strategies, and schedule.
- Analyze configuration and policy implementations and align them with corporate security policies and procedures, and Cisco best practices,
- Analyze security devices.
- Recommend tuning changes to policy and devices configurations.
- Recommend design or architecture reviews, if needed.
- Perform one (1) interactive tuning session with Customer to implement tuning recommendations.
- Provide an informal (email) summary of key findings, tuning recommendations, and tuning performed. An additional unit of Security Performance Tuning Support will be charged to the Customer in the event formal documentation is requested.

Limitations:

Security Performance Tuning Support is not intended for complex-systems and solutions, such as:

- Cisco ISE environments
- Cisco Secure ACS deployments
- Network devices supporting complex 802.1x deployments

Each unit of Security Performance Tuning and Support includes:

- Up to one (1) solution set (e.g. firewall solution, VPN solution, intrusion prevention system) OR up to one (1) security device type (e.g. multi-purpose security devices supporting firewall, VPN, and IPS.
- For solution sets: Up to five (5) devices within given solution set for the first Security PTS unit.
- For solution sets: Up to five (5) additional devices for additional Security PTS units IF a new solution set is added. For example, if the Security PTS includes firewall and VPN solutions then two Security PTS units allows up to ten (10) firewall and/or VPN devices to be analyzed and tuned.
- For solution sets: Up to fifteen (15) additional devices for additional Security PTS units IF the solution set does not change. For example, if the Security PTS includes a VPN solution then two Security PTS units allows up to twenty (20) VPN devices to be analyzed and tuned.
- For security device type: up to two (2) security devices.
- Work may occur after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Security Performance Tuning Support Questionnaire.
- Meet with Cisco to review Security Performance Tuning Support Request Form
- Meet with Cisco to establish performance tuning requirements, strategies, and schedule.
- Provide electronic access to Cisco to devices such that analysis and tuning may be completed.
- Reviewing and authorizing Cisco's recommendations for tuning.
- Change management and scheduling of performance tuning.
- Assisting with interactive tuning session with Cisco to implement tuning recommendations.

Security Proactive Software Recommendations (OPT-SOS-PSR)

Specific Service Responsibilities of Cisco

Cisco will provide proactive software recommendations that evaluate the various Security Software versions against internal Cisco caveat databases. Cisco will be responsible for the following:

- Provide the Security PSR Questionnaire.
- Gather Customer provided Security Software information, feature, functionality and capability requirements.
- Review the new Security Software features requested by the Customer.
- Document all features to be included in the Security Software Recommendation
- Evaluate the installed Software releases and new versions for interoperability issues and the ability to support current and future business and technical requirements.
- Provide detailed report including known caveats to which Customer may be exposed and if possible, appropriate workarounds for current and future business and technical objectives.

Limitations:
Each unit of the Security Proactive Software Recommendation includes:

- Up to one (1) software recommendation for one (1) Cisco product.
- Up to three (3) feature set profiles, based on up to five (5) sample configurations for each profile, provided by customer as representatives of deployed products.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Security PSR questionnaire.
- Provide Cisco with sample configurations for the Software being reviewed.
- Provide Cisco with a network diagram showing the devices and their relationship to other equipment in the Customer network.
- Provide Cisco with a list of required new features that need to be supported by the software to be reviewed.
- Review and accept the list of features to be included in the recommendation as provide by Cisco.
- Review and approve the recommendation results if it meets all requirements of the customer.

Security Remote Knowledge Transfer (OPT-SOS-KTM)

Specific Service Responsibilities of Cisco

Cisco will consult with Customer to identify requirements and topics for informal training sessions. Remote Knowledge Transfer Sessions are:

- Delivered in English (other languages subject to availability),
- Delivered remotely for up to four (4) hours in length, with no labs and no printed course materials,
- Relevant to the Cisco products and technologies deployed in Customer's production Network.
- Formal knowledge transfer sessions focusing on best practices for operating, tuning, maintaining, and managing Cisco security solutions
- Informal technical updates on a topic that is mutually agreed upon and relevant to security technologies, and,
  - Chalk talks,
  - Shadowing and mentoring as needed to assist your staff in assuming responsibility for Cisco security solution,
- Ongoing consultation to answer questions as needed for 30 days after a deployment.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Provide details on desired/requested topics Customer wants to see covered during the knowledge transfer and mentoring sessions.
- Provide background information on the Customer participant skill sets for the knowledge transfer or mentoring sessions.
- Provide Customer facilities and equipment (such as conference rooms, white boards, projectors) and make them available to host the informal technical update sessions.

Security Strategy and Planning Support (OPT-SOS-SPS)

Specific Service Responsibilities of Cisco

Cisco will provide strategic and tactical guidance via a series of meetings or workshop around a Customer selected security topic followed by a workshop for up to three (3) days to work through the incubation and strategy process covering topics that may include but are not limited to security technologies, cloud, TrustSec and identity, IT GRC (Governance, Risk Management and Compliance), TeleWorking, management, data center and collaboration security. Cisco responsibilities include:

- Briefing Customer on the service and service options.
- Conduct a Customer pre-planning workshop.
- Conducting Customer planning workshop.
- Capture synopsis and recommendations from workshop.
- Post-workshop analysis.
- Conduct post-workshop follow-up meeting.
- Capture synopsis and final recommendations post-workshop meeting.
- Create Work Summary and submit for Customer Review

Limitations:
Each unit of Security Strategy and Planning Support includes:

- Up to three (3) major challenge areas.
- Up to three (3) meetings or one (1) full-day pre-workshop meeting.
- Up to three (3) days for an onsite, offsite, or TelePresence workshop.
- Up to three (3) follow-up meetings or one (1) full-day post-workshop meeting.
- Up to four (4) concurrent Cisco participants.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Ensure all key stakeholders participate in Cisco briefing on the service and service options.
- Ensure all key stakeholders participate in the Cisco conducted meetings and workshops.
- Prepare for workshop and provide detailed briefing with supporting facts.
- Review and approve the Work Summary Review.

Security Technology Readiness Assessment (OPT-SOS-TRA)

Specific Service Responsibilities of Cisco

Cisco will work with Customer to define the Customer's business, technical and operational requirements, analyzing implementation requirements for a new security solution and assess the readiness of Customer's Network devices, operations, security policies, and architecture to support the solution Cisco is responsible for the following:

- Deliver the STRA questionnaire at least seven (7) business days prior to design workshop.
- Conduct design workshop to review STRA questionnaire.
- Analyze implementation requirements for a new security technology and assess the readiness of Customer's infrastructure, operations, security policies, and architecture to support the solution.
- Develop Security Readiness Assessment Report to document findings and recommendations including recommendations for modifications to the network infrastructure and to configuration parameters for application performance and availability.
- Conduct an interactive meeting with the customer to review all findings and develop steps to address gaps to ensure that the environment is ready to support the new technology.

Limitations:
Each unit of Security Technology Readiness Assessment includes:

- Up to one (1) security technology (i.e. Cisco ISE, AnyConnect Remote VPN, 802.1x deployments)
- Up to two (2) network segments with a total of up to ten (10) customer device classes. A class is defined as a group of devices (i.e. firewalls or routers) with similar configurations.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Respond to STRA questionnaire at least two (2) business days prior to design workshop.

- Ensure that appropriate customer engineers and management participate in the design workshop.
- Actively participate in development of steps to address changes required to ensure the network is ready to support the new technology.

Security Validation and Testing Premier Support (OPT-SOS-PVTS)

Specific Service Responsibilities of Cisco

Cisco will consult with Customer via a series of meetings to develop a thorough understanding of Customer's solution-oriented testing goals and requirements Cisco will execute networking tests and report findings to Customer. Support may include, among other information, the following:

- Provide Customer with Request for Validation and Testing Support Questionnaire, and a sample report.
- Review the Request for Validation and Testing Support Questionnaire.
- Meet with Customer to discuss responses to the Request for Validation and Testing Support Questionnaire, which may include the goals, business and technical requirements, testing methodology, Cisco standard validation and testing deliverable document format.
- Create and review the Test Plan with Customer.
- Provide Customer with requirements including lab facility, equipment, software, cabling, and interface requirements.
- Execute Test Plan upon Customer acceptance of Test Plan and Testing Schedule.
- Perform and document Test Results Analysis.
- Review Validation and Testing Report with customer.
- Review Customer feedback.
- Finalize and submit Validation and Testing Report to Customer.
- Provide local support at the Cisco lab facility, as needed, during remote testing. For example: in the event of a cable or connector failing during testing, then Cisco is responsible for providing replacement cable or connector.
- Provide Lab facility, equipment, software, cables, connectors, etc. required to perform testing.

  Set-up Lab, including rack and stack of equipment, cabling of power and network connections, confirmation of power-on self-test of equipment, confirmation of software version, and initial device configurations.

Cisco will utilize the following services and lab equipment to deliver Security VTPS

- 320 to 400 hours of Expertise, Test Engineer
- 80 Hours of Program management
- Up to $1.5M GPL List of HW (Included)

Limitations:

Each unit of Security Validation and Testing Support includes:

- Up to two (2) weeks for methodology development
- Up to two (2) weeks for test plan development.
- Up to one (1) week for Cisco site test lab setup
- Up to two (2) weeks design validation testing.
- Up to one (1) week results analysis.

Most engagements are between eight (8) and ten (10) weeks.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Request for Validation and Testing Support Questionnaire, which may include information such as goals, business and technical requirements, desired features and functionality, network diagrams, desired test plan and success criteria, and desired testing methodology.
- Provide appropriate production device configurations, if needed, for testing.
- Provide a designated single point of contact with authority to approve decisions.
- Provide Customer support as needed for third-party or Cisco competitor products.
- Provide equipment (including shipping to Cisco lab) some third-party or Cisco competitor products.

Security Validation and Testing Support (OPT-SOS-VTS)

Specific Service Responsibilities of Cisco

Cisco will consult with Customer via a series of meetings to develop a thorough understanding of Customer's solution-oriented testing goals and requirements Cisco will execute networking tests and report findings to Customer. Support may include, among other information, the following:

- Provide Customer with Request for Validation and Testing Support Questionnaire, and a sample report.
- Review the Customer completed Request for Validation and Testing Support Questionnaire.
- Meet with Customer to discuss responses to the Request for Validation and Testing Support Questionnaire, which may include the goals, business and technical requirements, testing methodology, Cisco standard validation and testing deliverable document format.
- Create and review the Test Plan with Customer.
- Provide Customer with requirements including lab facility, equipment, software, cabling, and interface requirements.
- Execute Test Plan upon Customer acceptance of Test Plan and Testing Schedule.
- Perform and document Test Results Analysis.
- Review Validation and Testing Report with customer.
- Review Customer feedback.
- Finalize and submit Validation and Testing Report to Customer.

Limitations: On Customer Site / Location

- Equipment supplied by Customer.
- Up to one (1) week for testing setup.
- Up to two (2) weeks of lab execution.
- 200 hours of Expertise, Test Engineer.
- 40 Hours of Program management.
- T&E as needed.

Other limitations include:

- Security Validation and Testing Support is not offered in every geography or location.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Request for Validation and Testing Support Questionnaire, which may include information such as goals, business and technical requirements, desired features and functionality, network diagrams, desired test plan and success criteria, and desired testing methodology.
- Provide Lab facility, equipment, software, cables, connectors, etc. required to perform testing.
- Provide appropriate production device configurations, if needed, for testing.
- Set-up Lab, including rack and stack of equipment, cabling of power and network connections, confirmation of power-on self-test of equipment, confirmation of software version, and initial device configurations (in cases such as production deployment re-creations).
- Provide local support, as needed, during onsite and remote testing. For example: in the event of a cable or connector failing during testing, then customer is responsible for providing replacement cable or connector.
- Provide Customer support as needed for some third-party or Cisco competitor products.

Software Security Alert (OPT-SOS-SA)

Cisco will provide proactive analysis of the security advisories (PSIRTs) that Cisco generates when security issues are uncovered that may impact networks in which Cisco products operate and the necessary action to repair and/or protect the network from these issues. After Cisco publicly releases the security advisory, the assessment is delivered to the Customer via the Software Security Alert (SSA). Cisco will provide an analysis of the vulnerability and its resolution with regard to its possible impact on the Customer's Security solution.

- Analysis of how a Cisco Security Advisory may or may not affect Customer's Network,
- Recommendations to mitigate risk, and,
- List of affected or potentially affected Networking devices.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Provide Cisco with a designated contact to handle all Security related announcements.

Technical Account Manager (OPT-SOS-SFTAM) (Existing Sourcefire Customers Only)

Cisco will provide a network-consulting engineer (NCE), onsite or remote, as selected, that will act as the primary interface with the Customer. Technical Account Manager services may be comprised of any activities and deliverables offered through Cisco Security Optimization Services. The NCE may also provide custom reports to the Customer based on the output from the Sourcefire security solution. The NCE may review custom rules on the device(s) for performance and make recommendations based on Cisco recommended best practices

Specific Service Responsibilities of Cisco

Cisco is responsible for the following:

- Collect all relevant information necessary to perform applicable optimization services.
- Review Customer’s security goals and requirements.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Ensuring all relevant stakeholders attend the Cisco interactive presentation of findings, analysis, and recommendations.
- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco with providing support.
- Open cases with vendor’s technical assistance center (e.g. Cisco TAC).

Specific Advisory Service Details (CON-AS-SECADV)

This section provides the service details for the following Advisory services:

- Custom Threat Intelligence 1 Gbps (OPT-SOS ADV CTI-1)
- Custom Threat Intelligence 10 Gbps (OPT-SOS ADV CTI-10)
- Incident Response Retainer (OPT-SOS ADV IR)
- Security Consulting Services (OPT-SOS ADV SCS)
- Security Design Assessment (OPT-SOS ADV SDA)
- Security Ongoing Flexible Support (Security ADV OFS)

Custom Threat Intelligence 1 Gbps (OPT-SOS ADV CTI-1)

Cisco's Custom Threat Intelligence Service combines threat and networking intelligence to provide visibility into both internal and external indicators of compromise.

Specific Service Responsibilities of Cisco

- Perform Network discovery jointly with Customer, and assess data traffic throughput vs sensor performance.
- Provide and configure one (1) UCS C240 server (to be provided by Cisco for use during the term of Services).
- Provide support for the installation of one (1) CTI Sensor (deployed per Customer requirements)
- Using the installed CTI Sensor, collect, export, enrich, and analyze the Customer network data (80 common TCP/IP ipv4 and ipv6 protocols including IP, TCP, UDP, DNS, HTTP, and SIP, as necessary), and perform the following activities:
- Analyze network traffic for anomalies and indications of compromise to include but not limited communication events indicating possible data exfiltration and evidence of malware on the internal network.
    - Develop one (1) monthly (for up to three (3) consecutive months) high level Internal Cyber Threat Report based analysis of network traffic originating from the Customer network as identified through the collection of network data on the Customer network and further enriched through the use of Cisco CTI processes and tools per reporting period. The Cyber Threat Report will include: One (1) actionable set of spreadsheets per reporting period.
    - Provide the Internal Cyber Threat Report to Customer.
    - Conduct one (1) ninety (90) minute conference call per delivered report to read out the report contents and discuss questions that will be scheduled by the Cisco engineer and will take place at a date and time convenient to the Customer.
- Provide remote support for CTI sensor hardware and analysis software throughout Services duration.
- The Cisco Custom Threat Intelligence sensor will collect data for analysis at a 1Gbps rate.

Specific Service Responsibilities of the Customer

- Perform Network discovery jointly with Cisco.
- Provide the data center, at least one (1) span port, network tap, or other agreed upon method to connect CTI Sensors to Customer production network for the purpose of data collection.
- Provide (physical) installation of the CTI sensors at the applicable data center.
- Provide Cisco with the necessary access to the CTI sensor to complete remote installation of the analysis software.
- Assume responsibility for any damage to or loss or theft of the CTI sensor while in Customer's custody.
- Return the UCS C240 server to Cisco within 60 calendar days, as instructed by Cisco, upon the completion of Services.

Custom Threat Intelligence 10 Gbps (**OPT-SOS ADV CTI-10**)

Cisco's Custom Threat Intelligence Service combines threat and networking intelligence to provide visibility into both internal and external indicators of compromise.

Specific Service Responsibilities of Cisco

- Perform Network discovery jointly with Customer, and assess data traffic throughput vs sensor performance.
- Provide and configure one (1) UCS C240 server (to be provided by Cisco for use during the term of Services).
- Provide support for the installation of one (1) CTI Sensor (deployed per Customer requirements)
- Using the installed CTI Sensor, collect, export, enrich, and analyze the Customer network data (80 common TCP/IP ipv4 and ipv6 protocols including IP, TCP, UDP, DNS, HTTP, and SIP, as necessary), and perform the following activities:
- Analyze network traffic for anomalies and indications of compromise to include but not limited communication events indicating possible data exfiltration and evidence of malware on the internal network.
    - Develop one (1) monthly (for up to three (3) consecutive months) high level Internal Cyber Threat Report based analysis of network traffic originating from the Customer network as identified through the collection of network data on the Customer network and further enriched through the use of Cisco CTI processes and tools per reporting period. The Cyber Threat Report will include: One (1) actionable set of spreadsheets per reporting period.
    - Provide the Internal Cyber Threat Report to Customer.
    - Conduct one (1) ninety (90) minute conference call per delivered report to read out the report contents and discuss questions that will be scheduled by the Cisco engineer and will take place at a date and time convenient to the Customer.
- Provide remote support for CTI sensor hardware and analysis software throughout Services duration.
- The Cisco Custom Threat Intelligence sensor will collect data for analysis at a 10 Gbps rate.

Specific Service Responsibilities of the Customer

- Perform Network discovery jointly with Cisco.
- Provide the data center, at least one (1) span port, network tap, or other agreed upon method to connect CTI Sensors to Customer production network for the purpose of data collection.
- Provide (physical) installation of the CTI sensors at the applicable data center.
- Provide Cisco with the necessary access to the CTI sensor to complete remote installation of the analysis software.
- Assume responsibility for any damage to or loss or theft of the CTI sensor while in Customer's custody.
- Return the UCS C240 server to Cisco within 60 calendar days, as instructed by Cisco, upon the completion of Services.

Incident Response Retainer (**OPT-SOS ADV IR**)

Specific Service Responsibilities of Cisco

Cisco may provide any or all of the following Incident Response (IR) deliverables as part of the retainer: incident readiness activities, triage an incident, evaluate and recommend containment actions, provide technical support (e.g. analysis and forensics), and project manage/coordinate incidents if requested. Cisco will also perform a comprehensive review of Customer's IR Program strategy, or if no strategy exists, will work to develop an IR strategy to better position Customer to respond to each information security incident, including such matters as potentially determining the source of the incident or vulnerability, effectively responding to the incident, and mitigating the harm or damages that might result from the incident. Cisco responsibilities include:

- Assisting in response to an incident(s)
- Assisting in coordinating the response to the incident both internally and potentially externally
- Evaluation and/or creation of an Incident Response Program strategy

Limitations:
Given the variety of situations and issues that may be encountered, incidents may require a variety of services to compliment this service. For example, incidents may require specialized tools to provide deeper visibility or access into the network.

Other limitations include:

- There is no guarantee that root-cause analysis will result in a root-cause being identified or confirmed for an incident
- Reasonable efforts will be made to provide conclusive findings and an issue resolution plan.
- IR services can provide insight into deficiences of an IR strategy and a plan for resolving; however, executing the plan may require follow-on services.
- Work may occur after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) from within its organization to serve as a liaison to Cisco.
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Ensure access to Incident Response strategy information, to include processes and workflows, is made available to Cisco.

Security Consulting Services (OPT-SOS ADV SCS)

Specific Service Responsibilities of Cisco

Cisco Security Advisory Team delivers a broad range of security, risk, and compliance advisory services required to support secure operations of an enterprise or government agency. These services are sold as a flexible subscription in blocks of 160 hours, with Cisco's business development manager helping to define the service selection and number of subscription blocks required. The selected subscription blocks can be used for delivery of one or a combination of services listed below.

Security Services include:

- Security Strategy
- Application architecture assessment
- Blackbox or combined application penetration assessment
- SDLC Improvement
- Mobile application assessment
- Cloud application assessment
- Network architecture assessment
- Network penetration assessment
- Wireless assessment
- Physical security assessment
- Social engineering and Phishing assessments
- Red Team/Blue Team Exercises
- Program Development (security, vulnerability management, penetration testing, or application assessment program)
- Mobile Security Workshop
- Cloud Security Workshop

Risk Services include:

- IT Risk Assessment
- IT Maturity Assessment
- Assessment of Organizational Alignment to ISO 27001/27002, NIST 800-53, or other appropriate standards
- Third-party risk assessment
- Security and risk metrics support
- Risk program development
- Risk program assessment
- Third-party risk program development

Compliance Services Include:

- HIPAA and HITECH assessment
- PCI ASV Scanning
- PCI Readiness

Security Design Assessment (OPT-SOS ADV SDA)

The Security Design Assessment evaluates the capabilities of the network infrastructure to protect an identified business critical asset and provide a set of recommendations to remediate and or mitigate the identified security gaps for that business critical asset. The recommendations include improvements to topology, protocols, device configurations and security controls and is limited to one business critical asset and sampling of devices from one each of the following network areas: data center, internal network, perimeter network.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:
  - Key business critical assets list.
  - Assess specific threats to identified business critical assets.
  - Physical and logical network topology diagrams, including the location of the devices included in assessment.
  - Network architecture description.
  - Security policies, standards, and procedures.
  - Services that traverse the perimeter network.
  - Applications and services running over the network (VoIP, video streaming, terminal emulation, http, ftp, etc.).
  - High-level architecture of data center, internal servers, user host connectivity and Internet connectivity.
  - Network Management System architecture.
  - Empirical data necessary to develop Cisco Security Control Framework metrics.

Further details on the Security Design Assessment are described in the SDA specific Service Description at www.cisco.com/go/servicedescriptions/, incorporated herein by reference.

Security Ongoing Flexible Support (OPT-SOS ADV OFS)

Cisco will provide informal, Ongoing Flexible Support for incremental changes to the network security architecture. This flexible support may be applied to other work items within Security Optimization Service and 1 Unit is limited to 40 hours of assigned engineer's time. Cisco engineers will be assigned as work items are selected throughout the term of the service contract.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide Cisco with details around what type of support is needed when a request is made.