



## Security Description: Cisco Security Remote Management Services

### 1 Cisco Security Remote Management Services

This document describes the Cisco Security Remote Management Services as delivered by the Cisco Remote Operations Service (Cisco ROS) Service Delivery team. This service description is designed to provide the Customer with a baseline understanding of the activities, deliverables and service delivery processes that Cisco uses to deliver Cisco Security Remote Management Services. This service description is also designed to properly set the Customer's expectations regarding these services.

Cisco Security Remote Management Services include three underlying security services that may be purchased separately or in any combination. These three security service offerings include:

- Cisco Security Access Control Remote Management Service
- Cisco Security Intrusion Prevention Remote Management Service
- Cisco Security Virtual Private Network (VPN) Remote Management Service

The Cisco ROS Security Operations Center (SOC) provides remote network management and monitoring support for specific security components of the Customer's access control infrastructure, intrusion prevention infrastructure and VPN infrastructure, enabling the Customer to out-task security administration by utilizing Cisco's security personnel as well as Cisco's process-driven remote network management methodology. Cisco Security Remote Management Services are designed to provide Customers with an extended network security support staff with a core competency in Cisco Security advanced technologies. Other benefits of these services include:

- Enabling the Customer to re-capture IT support team capacity by utilizing the Cisco ROS Security Operations Center (SOC) as an extension of their IT security staff
- Reducing security risk by improving the Customer's awareness of and visibility into network security threats and vulnerabilities
- Tightening Change-Release-Configuration Management processes on the Customer's network infrastructure to help strengthen network integrity
- Providing the Customer with engineering recommendations from Cisco ROS security engineers that will help a Customer decide which tactical operational steps they should take to mitigate threats, address vulnerabilities and, over time, improve their overall network security posture

Cisco Security Remote Management Services are intended to supplement current support agreements for Cisco products and are only available where all Managed Components in the Customer's network are supported through a minimum of core services such as Cisco's SMARTnet, Cisco Services for IPS and Software Application Services. Cisco shall provide Cisco Security Remote Management Services 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 between the parties and that, additionally, acknowledges and agrees to the terms contained therein. Cisco will only provide support of Managed Components for which Service has been selected.

Please read this document carefully as it contains important information regarding one or more of the security services that you have purchased from Cisco.

**Direct Sale from Cisco.** If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

**Sale via Cisco Authorized Reseller.** If you have purchased these Services through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this

Service is 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/service-descriptions/](http://www.cisco.com/go/service-descriptions/).

**Related Documents:** The following documents posted at [www.cisco.com/go/service-descriptions/](http://www.cisco.com/go/service-descriptions/) should be read in conjunction with this Service Description and are incorporated into this Service Description by this reference:

- Cisco ROS Service Glossary of Terms
- Cisco ROS Supported Device List

## 2 Cisco Security Access Control Remote Management Service

The objective of Cisco Security Access Control Remote Management Service is to manage and monitor the identified security components of the Customer's access control infrastructure, targeting access policy administration and troubleshooting of Managed Components as the primary areas of focus of this service.

The following Managed Components are covered under the Cisco Security Access Control Remote Management Service:

- Managed Components within Customer's access control infrastructure as outlined in the Cisco ROS Supported Device List located at [www.cisco.com/go/service-descriptions/](http://www.cisco.com/go/service-descriptions/)
- Management Termination router (as needed, Cisco-provided depending on method of remote management connectivity to the Managed Components of the Customer's access control infrastructure)
- Cisco ROS Syslog Server (Cisco-provided for capturing and storing syslog data from Managed Components entitled under this service)

### 2.1 Incident Management for Cisco Security Access Control Remote Management Service

Incident Management is the process used by the Cisco SOC to identify Incidents and restore service or remediate declared incidents as quickly as possible and may involve implementing temporary work-arounds. The Cisco Security Operations Center (Cisco SOC) will proactively monitor for key events and thresholds on Managed Components in the Customer's access control network infrastructure. In the case of undetected events, Customers may declare an Incident by contacting the Cisco ROS Service Desk, communicating via telephone any high priority Incidents (system down, degraded performance, etc.). Low priority incidents should be reported to the Cisco ROS Service Desk via the Cisco ROS Web Portal.

Upon automatic detection or manual submission of an Incident to the Cisco ROS Service Desk, an Incident Ticket is created. The Cisco ROS Service Desk will coordinate with the Cisco SOC during the lifespan of the declared Incident. The Cisco ROS Service Desk is ultimately responsible for coordinating the management of the Incident which includes communicating with the Customer throughout the Incident management process. This communication also includes notification to the Customer that the Incident has been resolved or remediated.

#### 2.1.1 Incident Detection

Cisco monitoring system indicates a fault condition, a performance threshold was exceeded, or a security event has triggered a security Incident.

Activities:

- Monitor (24x7x365) manageable elements of the Customer's network security infrastructure
- Perform ongoing Fault and Performance incident monitoring (re: alerting) on the entitled Managed Components of the Customer's network security infrastructure
- Perform ongoing Security incident monitoring (re: alerting) on the entitled Managed Components of the Customer's network security infrastructure.
- Detect Incidents
- Correlate Incidents where applicable

Deliverable(s):

- Confirmed Incidents logged in the Cisco ROS Configuration Management Database (CMDB)

### 2.1.2 Incident Record

Cisco ticketing system captures alarm / event / correlation data, enriches with relevant Configuration Item (CI) information and creates incident ticket.

Activities:

- Enrich alarm information with relevant Configuration Item (CI) information from the Cisco ROS CMDB

Deliverable(s):

- Create Incident Ticket
- Post Incident Ticket online via the Portal for the Customer to view all ticket handling activities and milestones

### 2.1.3 Incident Communication (E-notification)

Cisco will electronically notify (E-notify) designated Customer contacts for new Incidents or milestones achieved during the Incident Management process. E-notifications are sent to any email address or email-capable mobile device and will include the Incident Ticket number. The Customer (or its preferred vendor) can always view Incident status and detailed information via the Cisco ROS Web Portal.

Activities:

- Automated electronic notification (E-notification) to specific Customer contact(s) based on Customer's notification requirements as agreed on during the Service Activation process.
- Match customer's notification profile with Incident Ticket milestones

Deliverable(s):

- Perform E-notification of Incident Tickets per Customer's notification profile
- Log E-notification records in the Incident Ticket

### 2.1.4 Incident Priority and Classification

Incidents will be managed according to the Severity level as determined by IT Infrastructure Library (ITIL) service support framework. Incident Severity level depends on a variety of factors including pre-defined Incident Ticketing attributes such as business impact, urgency and asset value (if applicable and entered into Cisco's Configuration Management Database during the Service Activation phase). Incident Severity level will determine the Incident Priority level set by the Cisco SOC on a per-incident basis.

Activities:

- Evaluate Incident Severity and prioritize all Incidents into Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) Incident categories
- Classify Incidents into Fault, Performance or Security Incident categories

Deliverable(s):

- Properly prioritized Incidents based on Incident Ticketing attributes
- Report status prioritized Incident against its associated Service Level Objectives (SLO) as defined in the Service Level Management (SLM) section of this document

### 2.1.5 Incident Investigation and Diagnosis

Cisco SOC engineers utilize Incident Remediation procedures to collect any additional data required to fully diagnose and match the Incident to a known error in the Cisco ROS Knowledge Base (KB). Cisco SOC engineers will work to quickly isolate the root cause of the Incident. Once root cause isolation has occurred, Cisco SOC engineers will update the Incident Ticket with information related to root cause isolation and then proceed to the Incident resolution and restoration phase.

Activities:

- Collect additional data to properly diagnose root cause of the Incident
- Attempt to match Incident to a known error in the Cisco ROS Knowledge Base (KB)

Deliverable(s):

- Update Incident Ticket with root cause isolation information for Fault and Performance Incidents
- Update Incident Ticket with root cause security event information for Security Incidents
- Perform E-notification for this Incident Ticket event milestone (if requested by the Customer)

### **2.1.6 Incident Resolution and Restoration**

Cisco SOC engineers utilize Incident Remediation procedures and work to restore services within agreed service levels, initiating any Requests for Change (RFCs) as needed for restoration.

After the Incident has been isolated down to its root cause, Cisco SOC engineers will work to resolve the Incident. Resolution is complete when functionality is restored to the affected Managed Component(s) or, in the case of a Security Incident, a recommendation is made to the Customer to remediate the Incident. The resolution process includes any action the Cisco SOC requires to restore functionality to a Managed Component or remediate a Security Incident on the Customer's network infrastructure.

The Cisco SOC will utilize work-around solutions to restore all or partial functionality when full functionality cannot be restored within committed timeframes as defined in the Service Level Management section of this document. When a work-around is utilized, the Incident will continue to remain open and will be worked by Cisco SOC engineers until resolved, in accordance with the priority level of the Incident.

Incident resolution and restoration may include Cisco SOC security engineers working directly with the Customer's network IT team to resolve fault and performance incidents on the entitled Managed Components or to assist with the remediation of security incidents detected on the customer's network infrastructure. Cisco SOC security engineers may provide recommendations for remediation of an infected host (if detected). The Customer is ultimately responsible for any patching of infected hosts on their network.

Should the Cisco SOC require a configuration change in a Managed Component to resolve an issue or implement a work-around, the Cisco SOC will follow the Change Management Process established with the Customer

Activities:

- Resolve Fault and Performance Incidents on Managed Components
- Remediate Security Incidents on the Customer's network infrastructure
- Submit, when needed, a Cisco-recommended Request For Change (RFC) in accordance with the Change Management Process established with the Customer to tune benign traffic or implement a temporary work-around
- Dispatch third party vendors, as needed and appropriate, within the resolution steps prescribed by the Cisco SOC and in accordance with the Cisco SMARTnet or Cisco Services for IPS service terms on the affected Managed Components. As vendors are dispatched, the Incident Ticket will be updated with information related to the dispatch.
- Update Incident Ticket to include notes detailing Fault and Performance Incident resolution or recommendations for remediating Security Incidents.
- Perform E-notification for this Incident Ticket milestones, if requested by the Customer.

Deliverable(s):

- Updated Incident Ticket with resolution details on Faults and Performance related Incidents

- Updated Incident Ticket with recommendations detailing how to remediate a malicious Security Incident
- Updated Incident Ticket with justification for classifying benign Security Incidents
- Cisco-recommended Request for Change (RFC) for tuning a recurring benign Security Incident as determined by Cisco SOC engineers

#### 2.1.6.1 Incident Escalations

Escalation driven by elapsed time against SLOs ensuring effective routing of Incidents to appropriate technical resources as required. A Customer may request escalation of a Incident Ticket at any time via the Portal or Telephone telephone call to the Cisco ROS Service Desk. The Cisco SOC will refer Incidents to the Customer as needed and escalate the Incident with the Customer within the Customer's escalation guidelines until the Incident is resolved (ie: fault and performance incidents) or remediated (ie: security incidents).

Activities:

- Ensure Incident is being handled by appropriate Cisco SOC engineering resources to meet SLOs
- Escalate Incident as appropriate in the Cisco SOC or with the Customer per the established escalation procedures

Deliverable(s):

- Updated Incident Ticket to include escalation notes
- Incidents resolved or remediated in accordance with SLO targets
- Perform E-notification for this Incident Ticket event milestone, if requested by the Customer

#### 2.1.7 Incident Closure

Once the Cisco SOC declares an Incident resolved and verified, the incident will be closed. In the event that the Incident reoccurs, a new Incident Ticket will be created to accurately reflect the recurring nature of the Incident and aid in the identification of Problems. Depending on frequency, recurring Incidents may trigger the reactive Problem Management process which may include a Cisco-recommended Request For Change (RFC) to resolve the recurring Incident.

Any authorized Customer agent may also proactively request Incident Ticket closure via the Portal or Telephone. The Cisco SOC will review the request and work in conjunction with the Cisco ROS Service Desk to close the Incident Ticket or follow up with the Customer for more information as needed.

Activities:

- Confirm Incident is resolved
- If Incident reoccurs, depending on frequency and attributes of the Incident, open a Cisco-recommended RFC to resolve recurring Incident

Deliverable(s):

- Update Incident Ticket to include closing notes
- Close the Incident Ticket
- Perform E-notification for this Incident Ticket event milestone, if requested by the Customer.

## 2.2 Problem Management for Cisco Security Access Control Remote Management Service

The goal of Problem Management is to minimize the adverse impact of Incidents resulting from errors in the Customer's network by delivering a systematic approach for diagnosing the root causes of Incidents and preventing their reoccurrence by recommending the

elimination of the underlying errors whenever possible. To achieve this goal, Cisco SOC engineers will diagnose the root cause of Incidents and then initiate actions to improve or correct the situation.

### 2.2.1 Reactive Problem Management

Reactive problem management describes the problem management processes that primarily support incident management. These processes are initiated when an incident cannot be matched to a known error. A problem is declared for the purpose of tracking the activities that lead to identifying a root cause and a resolution to the incident's underlying error. The process concludes when a known error, including its root cause and resolution, has been identified and recorded in the Cisco ROS known error database. The known error will then be used to resolve and close all associated open and future incidents.

Activities:

- Utilize Problem Management procedures to collect additional data required to analyze the root cause
- Utilize error data, technical expertise, and product and development resources to isolate a root cause for the error
- Document recommended remediation and resolution procedures, and assist Incident Management team in the resolution of an error
- Error is closed and handed back to the Incident Management team for any further Incident Management activity

Deliverable(s):

- Faster Incident resolution for repetitive Incidents
- Accurate and updated known error database

Example:

- A Customer's network is running very slowly the Customer is speculating that their network may be infected by a worm or virus which is causing the network latency issue. The Cisco ROS Service Desk fields a call from the Customer requesting a Incident Ticket be opened manually. The Cisco ROS SOC engineer working the Incident escalates using the Problem Management process. A Cisco ROS SOC Problem Management engineer accesses the Customer's managed firewall, analyzes the current traffic patterns and matches the traffic to a new worm recently discovered in the wild. The Incident Ticket is updated with remediation procedures to enable the Customer to take specific action on remediating the worm activity and resolving the root cause of the network latency issue.

### 2.2.2 Proactive Problem Management

Proactive Problem Management prevents the occurrence or limits the adverse impact of future incidents. The Cisco SOC will analyze Incident trends to identify patterns and systemic conditions. In the event a trend is detected, the results will be introduced into the Problem Management process. The Cisco SOC analyzes different data sets based upon a variety of triggers that would indicate that a Managed Component should be further evaluated. Not all the aforementioned triggers are necessarily indicative of a problem requiring resolution.

Activities:

- Identify recurring Incidents and refer to Incident Management for resolution
- Analyze trends for Incidents on Managed Components
- Monitor the resolution
- Document applicable error, remediation, recovery, and resolution information in the Knowledge Base
- Perform annual configuration reviews for each qualified Managed Component on the Customer's access control infrastructure

Deliverables:

- Reduced number of errors in the customer's network

- Annual Configuration Review report on all Managed Components
- Improved network access control policies from actionable recommendations from the Annual Configuration Review report

Example:

- Cisco SOC Problem Management engineer performs a configuration review of a Customer's firewall and delivers a actionable list of recommendations to the Customer to tighten up their access control policy on the firewall to help reduce the risk of malicious security incidents

## 2.3 Change Management for Cisco Security Access Control Remote Management Service

Change Management is the process used by the Cisco SOC to apply standardized methods and procedures for authorizing, documenting, and performing all changes. The objective of Change Management is to make necessary Cisco-recommended and Customer-requested changes in an efficient and accountable manner, utilizing standard processes.

### 2.3.1 Change Origination

The first step in initiating the Change Management process is the origination of a Request for Change (RFC). RFCs may originate from two categories: Cisco-recommended changes and Customer-requested changes. Both changes are summarized in the tables below.

Cisco-Recommended Changes <sup>1</sup>		
Changes Required To:	Typically resulting in:	
Resolve an Incident or implement a work-around for an Incident	Logical or physical change	
Respond to a critical vulnerability or threat	Logical change	
Apply a software update to a entitled Managed Component	Logical change	
Resolve a known error identified during the Problem Management process	Logical or physical change	
Customer-Requested Changes		
Changes Required To:	Category	Change description
Add, Delete or Change physical component on existing Managed Component	Change	Physical change
Change existing logical functionality (Upgrades)	Change	Logical change
Physically move a Managed Component	Move	Physical move
Add a new Managed Component	Add	Physical add
Addition of new functionality <sup>2</sup>	Add	Logical add
Remove an existing Managed Component	Delete	Physical delete

<sup>1</sup> There will be no additional charges for any Cisco-Recommended changes

<sup>2</sup> Any Customer-requested Logical Change that results in the activation of additional functionality on a Managed Component will be evaluated on a case-by-case basis and discussed with the Customer. If Cisco determines that the additional functionality will increase service support requirements in the Cisco SOC the Customer may be asked to incur additional recurring monthly charges for Cisco SOC support of the additional functionality.

Activities:

- A Change Ticket is initiated by Cisco or the Customer

- The Change Ticket is categorized as described in the table above.
- The Customer tracks the progress of the change throughout its lifecycle.

Deliverable(s):

- Creation of a Change Ticket on the Cisco Portal for the Customer to view

### 2.3.1.1 Cisco-Recommended Changes

Cisco-recommended changes originate from the Cisco SOC. Before executing a Cisco-recommended change, the Cisco SOC will evaluate the change and make a recommendation to the Customer that will include details regarding the criticality and timeframe for implementation of the change. The Cisco SOC will not execute a change until the Customer has authorized or pre-authorized the change to be made.

Activities:

- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket.

#### 2.3.1.1.1 Cisco-recommended Changes required to resolve an Incident

During the course of the Incident management process, the Cisco SOC may decide to make changes to Managed Components in order to resolve Incidents. These changes are typically logical changes to access control Managed Component configurations for the purpose of troubleshooting and implementing temporary workarounds, and can also include changes to enable troubleshooting issues with third party vendors.

Changes required to resolve Incidents are implemented as needed by the Cisco SOC in accordance with agreed upon Change Management processes established with the Customer.

Activities:

- Logical configuration changes to implement a temporary work-around or aid in troubleshooting an Incident during the Incident Management process including logging level changes
- Logical configuration changes to apply software updates during the Incident Management process or the normal service support activities associated the Service and the entitled Managed Components
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket

Example:

- The Cisco SOC recommends an access control list (ACL) configuration change to a router to block network access for an attack source.

#### 2.3.1.1.2 Cisco-recommended Changes to respond to a critical Vulnerability or Threat

Cisco recognizes that certain critical vulnerabilities have the capability to degrade a Customer's system and severely limit network services. As new vulnerabilities are released or threats become known, the Cisco SOC will evaluate the severity and potential impact to the entitled managed component(s) of the Customer's access control infrastructure. If the vulnerability or threat is judged by the Cisco SOC to be critical with respect to Customer safeguards, or the Customer is impacted by the vulnerability, the Cisco SOC will recommend changes to correct the issue and/or mitigate the threat. If requested by the Customer, changes will be executed according to the priorities and terms contained in Customer-Requested Change section of this service description.

Changes to address critical vulnerabilities will be performed at the earliest possible time, in coordination with Customer and the agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to respond to a critical vulnerability or threat identified by the Cisco SOC
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket.

Example:

- The Cisco SOC recommends upgrading the operating system (OS) of a managed firewall appliance that the Cisco Product Security Incident Response Team (PSIRT) has recently identified as having a critical vulnerability.

#### 2.3.1.1.3 Cisco-recommended Changes to address known errors uncovered during the Problem Management process

During the course of the Problem Management process, the Cisco SOC may recommend changes to the Managed Components of the Customer's access control infrastructure in order to resolve a known error. Changes required to resolve known errors are implemented as needed by the Cisco SOC in accordance with agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to resolve a known error identified during the Problem Management process
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process

Example:

- A Cisco SOC engineer recommends a configuration change on a Customer's firewall to allow a particular port and protocol that will enable a Customer's business application to function on their network as required.

### 2.3.2 Customer-Requested Changes

Customer-requested changes are changes that originate with the Customer. The Customer can use the Cisco Portal to submit Customer-requested changes. This will automatically initiate the Change Management process. The Customer can also call the Cisco ROS Service Desk and describe the change request over the phone. The Cisco ROS Service Desk will make the initial evaluation of the Request For Change (RFC) and coordinate with the Cisco SOC Change Manager in compliance with the agreed upon Change Management process established between Cisco and the Customer.

A Change Management process that includes costs, timeframes, and guidelines for the work to be completed is based on the classifications of the RFC and governs all Customer-requested changes. These guidelines ensure that the Cisco SOC receives proper notice (re: lead time) to arrange the required resources to complete the work in an expeditious manner. The specifics of the Change Management Process, including any additional costs, are outlined and reviewed with the Customer during the Service Activation phase.

The Cisco SOC Change Manager evaluates the potential impact of Customer-requested changes and will determine if a Cisco security engineer will need to discuss the implications of a requested change with the Customer. If the Cisco SOC Change Manager determines that the change requires additional information, planning, diligence or testing, the Cisco SOC Change Manager will coordinate the Cisco SOC Change Advisory Board (CAB) which may, in their discretion, refuse the Customer-requested change if they determine that the change will adversely affect the functionality of the entitled Managed Components or the security posture of the Customer's access control infrastructure. The Cisco SOC Change Manager will have responsibility for communicating acceptance or rejection of the Request for Change (RFC).

## Activities:

- Cisco ROS Service Desk makes initial evaluation of the RFC and coordinates with the Cisco SOC Change Manager
- Cisco SOC Change Manager classifies the change into one of the following categories: Move, Add, Change, Delete or Project
- Cisco SOC Change Manager coordinates with the Cisco SOC Change Advisory Board (CAB) as needed to determine the level-of-effort and business risk associated to the change request as defined in the IT Infrastructure Library (ITIL) Change Management framework under the following change categories: Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or a designated member of the Cisco SOC CAB communicates with the Customer regarding the criticality and timeframe associated to the change in accordance with the change attributes
- Cisco SOC Change Manager obtains approval from the Customer for executing the change
- Cisco SOC follows the established Change Management process including updating all activities in the Change Ticket

**2.3.2.1 Customer-requested Change - Logical**

A Logical Change includes changes to software on Managed Components of the Customer's access control infrastructure. Logical Changes requiring an increased level of planning, involving multiple Managed Components or requiring more than four hours of work will typically be treated as a Project. The Cisco SOC Change Manager will have the responsibility of determining the level-of-effort to support the Logical Change request and if it should be treated as a Project.

## Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

## Example:

- The Customer is adding a new server to their DMZ and needs configuration changes on a firewall to allow access to the server

**2.3.2.2 Customer-requested Change - Physical**

A Physical Change is a change to a hardware element on an existing Managed Component such as a network module. The installation portion of a Physical Change may involve loading and verification of the new Managed Component information into the Cisco ROS Configuration Management Database (CMDB). The configuration portion of a Physical Change includes logical configuration changes targeting proper functionality of the Managed Component.

## Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

## Example:

- The Customer submits an RFC to add a network interface card (NIC) to their existing managed firewall.

**2.3.2.3 Customer-requested Move - Physical**

A Physical Move is a change required to physically move a Managed Component of the Customer's access control infrastructure from one location to another. For a Physical Move, the Customer or a qualified Cisco Partner is responsible for physically moving the component from one location to the next. Cisco is responsible for making the necessary changes in the Cisco ROS CMDB and the configuration of the Managed Component so that management can continue in the new physical location. The Cisco SOC will work with the Customer to coordinate the Physical Move and re-establish remote management connectivity to the Managed Component.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to ensure that a managed firewall and router are brought back under Cisco SOC management once the devices are physically moved and plugged back in at a new physical location.

#### **2.3.2.4 Customer-requested Add - Physical**

A Physical Add is the addition of new Managed Component(s) entitled under the Cisco Security Access Control Remote Management Service. A data-gathering process involving verification and loading of all Managed Component information in the Cisco ROS CMDB including serial numbers, maintenance contract information, circuit information, Carrier information, and more (as needed).

The Managed Component configuration process includes logical configuration changes to ensure that the new Managed Component can be properly managed.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to add a failover firewall appliance to their access control infrastructure

#### **2.3.2.5 Customer-requested Add – Logical**

Logical Adds include installation of new software on Managed Components of the Customer's Access Control infrastructure to enhance or introduce new services or functionality. Logical Adds do not require a high degree of planning and implications for other Managed Components. If the additional functionality introduces new services to other Managed Components or end users, or if the functionality requires extensive planning, the Logical Add may be treated as a Project and thus incur additional fees billed at the Cisco ROS professional services rate.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to enable the web filtering feature available on their managed firewall.

#### **2.3.2.6 Customer-requested Delete – Logical**

Logical Deletes refer to removing a Managed Component from the Cisco Security Access Control Remote Management Service so that it is no longer a Managed Component. The Managed Component may or may not still exist in the Customer's network.

A Logical Delete requiring a Cisco security engineer to make modifications to the Customer's access control infrastructure to allow the Managed Component to be removed (such as transferring functionality to another Managed Component, modifying access control lists, routing, etc.) will be considered a Project if the Cisco SOC Change Manager determines the work required will exceed 4 hours of engineering time.

## Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

## Example:

- The Customer submits an RFC to terminate the Cisco Security Access Control Remote Management Service on a managed firewall appliance. The firewall will remain on the Customer's network.

**2.3.2.7 Customer-requested Delete – Physical**

A Physical Delete requires a Cisco SOC security engineer to make modifications to the Customer's network infrastructure to allow the Managed Component to be physically removed or replaced by another Managed or Non-Managed Component on the Customer's network (i.e., transferring functionality from one Managed Component to another Managed or Non-Managed Component). Any transfer of functionality from a Managed Component to a Non-Managed Component will be the primary responsibility of the Customer.

## Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

## Example:

- The Customer submits an RFC to decommission a PIX firewall at a remote site and transfer access control functionality to an existing router currently deployed on the perimeter of their network.

**2.3.2.8 Customer-requested Projects**

Customer-requested Changes that have one or more of the following attributes typically will be handled as a Project:

- Introduction of a service or functionality that is not currently being used in the Customer's network.
- Cisco SOC engineering work required to support the request exceeds four hours.
- Significant planning is required before implementation of the change request.
- Logical Change involves changes to multiple Managed Components at the same time.

## Activities:

- Cisco SOC Change Manager will assess the scope of the project, coordinate the Cisco ROS CAB, and build out a Statement of Work (SOW) to present to the Customer for acceptance or rejection (as Professional Services fees will normally apply)
- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

## Example:

- The Customer submits an RFC for an operating system (OS) upgrade involving 10 managed firewall appliances in order to take advantage of new key functionality in the upgraded version of OS.

### **2.3.3 Executing changes**

After changes are executed, the Cisco SOC will notify the Customer that the change has been executed. Once the Customer accepts the change, the Ticket will be closed. The status of changes can be viewed on the Portal.

Activities:

- Maintain a ticket history of changes visible through the Portal
- Evaluate change requests
- Authorize and schedule change requests
- Coordinate changes.
- Update Portal Tickets to include change status.
- Review and close change requests.

Deliverable(s):

- Executed change.
- Portal Ticket updated with change notes.

### 3 Cisco Security Intrusion Prevention Remote Management Service

The objective of the Cisco Security Intrusion Prevention Remote Management Service is to manage and monitor the identified security components of the Customer's intrusion prevention infrastructure, targeting malicious network activity that may threaten a Customer's business and providing the Customer with a 24x7 Security incident handling, analysis and response capability.

The following Managed Components are covered under the Cisco Security Intrusion Prevention Remote Management Service:

- Managed Components within Customer's intrusion prevention infrastructure as outlined in the Cisco ROS Supported Device List located at [www.cisco.com/go/servicedescriptions/](http://www.cisco.com/go/servicedescriptions/)
- Management Termination router (as needed, Cisco-provided depending on method of remote management connectivity to the Managed Components of the Customer's intrusion prevention infrastructure)

#### 3.1 Incident Management for Cisco Security Intrusion Prevention Remote Management Service

Incident Management is the process used by the Cisco SOC to identify Incidents and restore service or remediate declared incidents as quickly as possible and may involve implementing temporary work-arounds. The Cisco Security Operations Center (Cisco SOC) will proactively monitor for key events and thresholds on Managed Components in the Customer's intrusion prevention infrastructure. In the case of undetected events, Customers may declare an Incident by contacting the Cisco ROS Service Desk, communicating via telephone any high priority Incidents (system down, degraded performance, etc.). Low priority incidents should be reported to the Cisco ROS Service Desk via the Cisco ROS Web Portal.

Upon automatic detection or manual submission of an Incident to the Cisco ROS Service Desk, an Incident Ticket is created. The Cisco ROS Service Desk will coordinate with the Cisco SOC during the lifespan of the declared Incident. The Cisco ROS Service Desk is ultimately responsible for coordinating the management of the Incident which includes communicating with the Customer throughout the Incident management process. This communication also includes notification to the Customer that the Incident has been resolved or remediated.

##### 3.1.1 Incident Detection

Cisco monitoring system indicates a fault condition, a performance threshold was exceeded, or a security event has triggered a security Incident.

Activities:

- Monitor (24x7x365) manageable elements of the Customer's network security infrastructure
- Perform ongoing Fault and Performance incident monitoring (re: alerting) on the entitled Managed Components of the Customer's network security infrastructure
- Perform ongoing Security incident monitoring (re: alerting) on the entitled Managed Components of the Customer's network security infrastructure.
- Detect Incidents
- Correlate Incidents where applicable

Deliverable(s):

- Confirmed Incidents logged in the Cisco ROS Configuration Management Database (CMDB)

##### 3.1.2 Incident Record

Cisco ticketing system captures alarm / event / correlation data, enriches with relevant Configuration Item (CI) information and creates incident ticket

Activities:

- Enrich alarm information with relevant Configuration Item (CI) information from the Cisco ROS CMDB

Deliverable(s):

- Create Incident Ticket
- Post Incident Ticket online via the Portal for the Customer to view all ticket handling activities and milestones

### 3.1.3 Incident Communication (E-notification)

Cisco will electronically notify (E-notify) designated Customer contacts for new Incidents or milestones achieved during the Incident Management process. E-notifications are sent to any email address or email-capable mobile device and will include the Incident Ticket number. The Customer (or its preferred vendor) can always view Incident status and detailed information via the Cisco ROS Web Portal.

Automated electronic notification (E-notification) to specific Customer contact(s) based on Customer's notification requirements as agreed on during the Service Activation process.

Activities:

- Match customer's notification profile with Incident Ticket milestones

Deliverable(s):

- Perform E-notification of Incident Tickets per Customer's notification profile
- Log E-notification records in the Incident Ticket

### 3.1.4 Incident Priority and Classification

Incidents will be managed according to the Severity level as determined by IT Infrastructure Library (ITIL) service support framework. Incident Severity level depends on a variety of factors including pre-defined Incident Ticketing attributes such as business impact, urgency and asset value (if applicable and entered into Cisco's Configuration Management Database during the Service Activation phase). Incident Severity level will determine the Incident Priority level set by the Cisco SOC on a per-incident basis.

Activities:

- Evaluate Incident Severity and prioritize all Incidents into Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) Incident categories
- Classify Incidents into Fault, Performance or Security Incident categories

Deliverable(s):

- Properly prioritized Incidents based on Incident Ticketing attributes
- Report status prioritized Incident against its associated Service Level Objectives (SLO) as defined in the Service Level Management (SLM) section of this document

### 3.1.5 Incident Investigation and Diagnosis

Cisco SOC engineers utilize Incident Remediation procedures to collect any additional data required to fully diagnose and match the Incident to a known error in the Cisco ROS Knowledge Base (KB). Cisco SOC engineers will work to quickly isolate the root cause of the Incident. Once root cause isolation has occurred, Cisco SOC engineers will update the Incident Ticket with information related to root cause isolation and then proceed to the Incident resolution and restoration phase.

Activities:

- Collect additional data to properly diagnose root cause of the Incident
- Attempt to match Incident to a known error in the Cisco ROS Knowledge Base (KB)

## Deliverable(s):

- Update Incident Ticket with root cause isolation information for Fault and Performance Incidents
- Update Incident Ticket with root cause security event information for Security Incidents
- Perform E-notification for this Incident Ticket event milestone (if requested by the Customer)
- Security events will be root caused to one of the following: Attack, Successful Attack, Probable Attack, Reconnaissance, Misuse, Worm, Virus, or Benign

## Example:

- Internal gaming activity on the Customer's network is detected by a Managed Component and isolated with a root cause of "Misuse" by the Cisco SOC.

**3.1.6 Incident Resolution and Restoration**

Cisco SOC engineers utilize Incident Remediation procedures and work to restore services within agreed service levels, initiating any Requests for Change (RFCs) as needed for restoration.

After the Incident has been isolated down to its root cause, Cisco SOC engineers will work to resolve the Incident. Resolution is complete when functionality is restored to the affected Managed Component(s) or, in the case of a Security Incident, a recommendation is made to the Customer to remediate the Incident. The resolution process includes any action the Cisco SOC requires to restore functionality to a Managed Component or remediate a Security Incident on the Customer's network infrastructure.

The Cisco SOC will utilize work-around solutions to restore all or partial functionality when full functionality cannot be restored within committed timeframes as defined in the Service Level Management section of this document. When a work-around is utilized, the Incident will continue to remain open and will be worked by Cisco SOC engineers until resolved, in accordance with the priority level of the Incident.

Incident resolution and restoration may include Cisco SOC security engineers working directly with the Customer's network IT team to resolve fault and performance incidents on the entitled Managed Components or to assist with the remediation of security incidents detected on the customer's network infrastructure. Cisco SOC security engineers may provide recommendations for remediation of an infected host (if detected). The Customer is ultimately responsible for any patching of infected hosts on their network.

Should the Cisco SOC require a configuration change in a Managed Component to resolve an issue or implement a work-around, the Cisco SOC will follow the Change Management Process established with the Customer

## Activities:

- Resolve Fault and Performance Incidents on Managed Components
- Remediate Security Incidents on the Customer's network infrastructure
- Submit, when needed, a Cisco-recommended Request For Change (RFC) in accordance with the Change Management Process established with the Customer to tune benign traffic or implement a temporary work-around
- Dispatch third party vendors, as needed and appropriate, within the resolution steps prescribed by the Cisco SOC and in accordance with the Cisco SMARTnet or Cisco Services for IPS service terms on the affected Managed Components. As vendors are dispatched, the Incident Ticket will be updated with information related to the dispatch
- Update Incident Ticket to include notes detailing Fault and Performance Incident resolution or recommendations for remediating Security Incidents.
- Perform E-notification for this Incident Ticket milestones, if requested by the Customer

## Deliverable(s):

- Updated Incident Ticket with resolution details on Faults and Performance related Incidents
- Updated Incident Ticket with recommendations detailing how to remediate a malicious Security Incident

- Updated Incident Ticket with justification for classifying benign Security Incidents
- Cisco-recommended Request for Change (RFC) for tuning a recurring benign Security Incident as determined by Cisco SOC engineers

Example:

- An internal worm infection is isolated on the Customer's network and the recommendation to block port 443 on the customer's Internet-facing router to prevent further infection is made. Additionally, a recommendation from Cisco SOC to the Customer is made regarding upgrading all potentially vulnerable Windows servers to the latest Service Pack release.

### 3.1.6.1 Incident Escalations

Escalation driven by elapsed time against SLOs ensuring effective routing of Incidents to appropriate technical resources as required. A Customer may request escalation of a Incident Ticket at any time via the Portal or Telephone telephone call to the Cisco ROS Service Desk. The Cisco SOC will refer Incidents to the Customer as needed and escalate the Incident with the Customer within the Customer's escalation guidelines until the Incident is resolved (ie: fault and performance incidents) or remediated (ie: security incidents).

Activities:

- Ensure Incident is being handled by appropriate Cisco SOC engineering resources
- Escalate Incident as appropriate in the Cisco SOC or with the Customer per the established escalation procedures

Deliverable(s):

- Updated Incident Ticket to include escalation notes
- Incidents resolved or remediated in accordance with SLO targets
- Perform E-notification for this Incident Ticket event milestone, if requested by the Customer

Example:

- An Intrusion Prevention device fault is detected. The fault is troubleshot by the Tier 1 Incident Management team in the Cisco SOC but the SLO is in danger of not being met. The fault is escalated to Tier 2 or Tier 3 Cisco SOC engineers to resolve the fault condition as quickly as possible.

### 3.1.7 Incident Closure

Once the Cisco SOC declares an Incident resolved and verified, the incident will be closed. In the event that the Incident reoccurs, a new Incident Ticket will be created to accurately reflect the recurring nature of the Incident and aid in the identification of Problems. Depending on frequency, recurring Incidents may trigger the reactive Problem Management process which may include a Cisco-recommended Request For Change (RFC) to resolve the recurring Incident.

Any authorized Customer agent may also proactively request Incident Ticket closure via the Portal or Telephone. The Cisco SOC will review the request and work in conjunction with the Cisco ROS Service Desk to close the Incident Ticket or follow up with the Customer for more information as needed.

Activities:

- Confirm Incident is resolved
- If Incident reoccurs, depending on frequency and attributes of the Incident, open a Cisco-recommended RFC to resolve recurring Incident

Deliverable(s):

- Update Incident Ticket to include closing notes

- Close the Incident Ticket
- Perform E-notification for this Incident Ticket event milestone, if requested by the Customer.

### 3.2 Problem Management for Cisco Security Intrusion Prevention Remote Management Service

The goal of Problem Management is to minimize the adverse impact of Incidents resulting from errors in the Customer's network by delivering a systematic approach for diagnosing the root causes of Incidents and preventing their reoccurrence by recommending the elimination of the underlying errors whenever possible. To achieve this goal, Cisco SOC engineers will diagnose the root cause of Incidents and then initiate actions to improve or correct the situation.

#### 3.2.1 Reactive Problem Management

Reactive problem management describes the problem management processes that primarily support incident management. These processes are initiated when an incident cannot be matched to a known error. A problem is declared for the purpose of tracking the activities that lead to identifying a root cause and a resolution to the incident's underlying error. The process concludes when a known error, including its root cause and resolution, has been identified and recorded in the known error database. The known error will then be used to resolve and close all associated open and future incidents.

Activities:

- Utilize Problem Management procedures to collect additional data required to analyze the root cause
- Utilize error data, technical expertise, and product and development resources to isolate a root cause for the error
- Document recommended remediation and resolution procedures, and assist Incident Management team in the resolution of an error
- Error is closed and handed back to the Incident Management team for any further Incident Management activity

Deliverable(s):

- Faster Incident resolution for repetitive Incidents
- Accurate and updated known error database

Example:

- A Customer's non-managed component (re: network host) is infected a second time with a virus. Because there is already an existing known error in the Cisco ROS Knowledge Base that details this security Incident, the Cisco SOC is able to resolve this Incident much faster than it took to resolve the first occurrence of the Incident.

#### 3.2.2 Proactive Problem Management

Proactive Problem Management prevents the occurrence or limits the adverse impact of future incidents. The Cisco SOC will analyze Incident trends to identify patterns and systemic conditions. In the event a trend is detected, the results will be introduced into the Problem Management process. The Cisco SOC analyzes different data sets based upon a variety of triggers that would indicate that a Managed Component should be further evaluated. Not all the aforementioned triggers are necessarily indicative of a problem requiring resolution.

Activities:

- Identify recurring Incidents and refer to Incident Management for resolution
- Analyze trends for Incidents on Managed Components
- Monitor the resolution
- Document applicable error, remediation, recovery, and resolution information in the Knowledge Base

Deliverables:

- Reduce the number of errors in the Customer's network

Example:

- Cisco SOC Problem Management engineering resources perform a trend analysis on a particular Intrusion Prevention System (IPS) signature and discover a high rate of benign triggering. Cisco SOC Problem Management engineering resources communicate this to the Cisco Signature Engineering team to build a new IPS signature pack to reduce the frequency of the benign trigger.

### 3.3 Change Management for Cisco Security Intrusion Prevention Remote Management Service

Change Management is the process used by the Cisco SOC to apply standardized methods and procedures for authorizing, documenting, and performing all changes. The objective of Change Management is to make necessary Cisco-recommended and Customer-requested changes in an efficient and accountable manner, utilizing standard processes.

#### 3.3.1 Change Origination

The first step in initiating the Change Management process is the origination of a Request for Change (RFC). RFCs may originate from two categories: Cisco-recommended changes and Customer-requested changes. Both changes are summarized in the tables below.

Cisco-Recommended Changes <sup>1</sup>		
Changes Required To:	Typically resulting in:	
Resolve an Incident or implement a work-around for an Incident	Logical or physical change	
Respond to a critical vulnerability or threat	Logical change	
Apply a software update to a entitled Managed Component	Logical change	
Resolve a known error identified during the Problem Management process	Logical or physical change	
Customer-Requested Changes		
Changes Required To:	Category	Change description
Add, Delete or Change physical component on existing Managed Component	Change	Physical change
Change existing logical functionality (Upgrades)	Change	Logical change
Physically move a Managed Component	Move	Physical move
Add a new Managed Component	Add	Physical add
Addition of new functionality <sup>2</sup>	Add	Logical add
Remove an existing Managed Component	Delete	Physical delete

<sup>1</sup> There will be no additional charges for any Cisco-Recommended changes

<sup>2</sup> Any Customer-requested Logical Change that results in the activation of additional functionality on a Managed Component will be evaluated on a case-by-case basis and discussed with the Customer. If Cisco determines that the additional functionality will increase service support requirements in the Cisco SOC the Customer may be asked to incur additional recurring monthly charges for Cisco SOC support of the additional functionality.

## Activities:

- A Change Ticket is initiated by Cisco or the Customer
- The Change Ticket is categorized as described in the table above.
- The Customer tracks the progress of the change throughout its lifecycle.

## Deliverable(s):

- Creation of a Change Ticket on the Cisco Portal for the Customer to view

**3.3.1.1 Cisco-Recommended Changes**

Cisco-recommended changes originate from the Cisco SOC. Before executing a Cisco-recommended change, the Cisco SOC will evaluate the change and make a recommendation to the Customer that will include details regarding the criticality and timeframe for implementation of the change. The Cisco SOC will not execute a change until the Customer has authorized or pre-authorized the change to be made.

## Activities:

- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket

## Example:

- Cisco SOC recommends a IPS signature pack upgrade to ensure the latest IPS signatures are active on the Customer's Managed Component (re: IPS appliance).

**3.3.1.1.1 Cisco-recommended Changes required to resolve an Incident**

During the course of the Incident management process, the Cisco SOC may decide to make changes to Managed Components in order to resolve Incidents. These changes are typically logical changes to access control Managed Component configurations for the purpose of troubleshooting and implementing temporary workarounds, and can also include changes to enable troubleshooting issues with third party vendors.

Changes required to resolve Incidents are implemented as needed by the Cisco SOC in accordance with agreed upon Change Management processes established with the Customer.

## Activities:

- Logical configuration changes to implement a temporary work-around or aid in troubleshooting an Incident during the Incident Management process including logging level changes
- Logical configuration changes to apply software updates during the Incident Management process or the normal service support activities associated the Service and the entitled Managed Components
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket

## Example:

- The Cisco SOC determines that the Intrusion Prevention System (IPS) appliance is accidentally blocking legitimate network traffic on the Customer's network due to a change in the most recent IPS Signature Pack release. The Cisco SOC recommends a configuration change to the IPS appliance to always allow traffic from a particular trusted source IP.

### 3.3.1.1.2 Cisco-recommended Changes to respond to a critical Vulnerability or Threat

Cisco recognizes that certain critical vulnerabilities have the capability to degrade a Customer's system and severely limit network services. As new vulnerabilities are released or threats become known, the Cisco SOC will evaluate the severity and potential impact to the entitled managed component(s) of the Customer's access control infrastructure. If the vulnerability or threat is judged by the Cisco SOC to be critical with respect to Customer safeguards, or the Customer is impacted by the vulnerability, the Cisco SOC will recommend changes to correct the issue and/or mitigate the threat. If requested by the Customer, changes will be executed according to the priorities and terms contained in Customer-Requested Change section of this service description.

Changes to address critical vulnerabilities will be performed at the earliest possible time, in coordination with Customer and the agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to respond to a critical vulnerability or threat identified by the Cisco SOC
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket

Example:

- A Cisco Product Security Incident Response Team (PSIRT) advisory is released to the public detailing a vulnerability on a particular model and version of the Cisco Intrusion Prevention System (IPS) appliance. The Cisco SOC initiates an RFC and coordinates with the Customer to update the Operating System (OS) on the IPS appliance.

### 3.3.1.1.3 Cisco-recommended Changes to address known errors uncovered during the Problem Management process

During the course of the Problem Management process, the Cisco SOC may recommend changes to the Managed Components of the Customer's access control infrastructure in order to resolve a known error.

Changes required to resolve known errors are implemented as needed by the Cisco SOC in accordance with agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to resolve a known error identified during the Problem Management process
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process.

Example:

- During the Problem Management process a Cisco ROS SOC engineer uncovers a known error for a benign trigger caused by a particular application that several Cisco ROS customers are running on their respective networks. The Cisco ROS SOC initiates an RFC for each Customer and works with each Customer to tune the Customers' Intrusion Prevention System appliances and eliminate the false positive condition.

## 3.3.2 Customer-Requested Changes

Customer-requested changes are changes that originate with the Customer. The Customer can use the Cisco Portal to submit Customer-requested changes. This will automatically initiate the Change Management process. The Customer can also call the Cisco ROS Service Desk and describe the change request over the phone. The Cisco ROS Service Desk will make the initial evaluation of the Request For Change (RFC) and coordinate with the Cisco SOC Change Manager in compliance with the agreed upon Change Management process established between Cisco and the Customer.

A Change Management process that includes costs, timeframes, and guidelines for the work to be completed is based on the classifications of the RFC and governs all Customer-requested changes. These guidelines ensure that the Cisco SOC receives proper

notice (re: lead time) to arrange the required resources to complete the work in an expeditious manner. The specifics of the Change Management Process, including any additional costs, are outlined and reviewed with the Customer during the Service Activation phase.

The Cisco SOC Change Manager evaluates the potential impact of Customer-requested changes and will determine if a Cisco security engineer will need to discuss the implications of a requested change with the Customer. If the Cisco SOC Change Manager determines that the change requires additional information, planning, diligence or testing, the Cisco SOC Change Manager will coordinate the Cisco SOC Change Advisory Board (CAB) which may, in their discretion, refuse the Customer-requested change if they determine that the change will adversely affect the functionality of the entitled Managed Components or the security posture of the Customer's access control infrastructure. The Cisco SOC Change Manager will have responsibility for communicating acceptance or rejection of the Request for Change (RFC).

Activities:

- Cisco ROS Service Desk makes initial evaluation of the RFC and coordinates with the Cisco SOC Change Manager
- Cisco SOC Change Manager classifies the change into one of the following categories: Move, Add, Change, Delete or Project
- Cisco SOC Change Manager coordinates with the Cisco SOC Change Advisory Board (CAB) as needed to determine the level-of-effort and business risk associated to the change request as defined in the IT Infrastructure Library (ITIL) Change Management framework under the following change categories: Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or a designated member of the Cisco SOC CAB communicates with the Customer regarding the criticality and timeframe associated to the change in accordance with the change attributes
- Cisco SOC Change Manager obtains approval from the Customer for executing the change
- Cisco SOC follows the established Change Management process including updating all activities in the Change Ticket

### 3.3.2.1 Customer-requested Change - Logical

A Logical Change includes changes to software on Managed Components of the Customer's access control infrastructure. Logical Changes requiring an increased level of planning, involving multiple Managed Components or requiring more than four hours of work will typically be treated as a Project. The Cisco SOC Change Manager will have the responsibility of determining the level-of-effort to support the Logical Change request and if it should be treated as a Project.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer is deploying a new application in their network and wants to ensure this traffic is not going to be blocked by the IPS appliance. The Customer asks the Cisco SOC to update the IPS configuration to include a filter to always allow this particular traffic.

### 3.3.2.2 Customer-requested Change - Physical

A Physical Change is a change to a hardware element on an existing Managed Component such as a network module. The installation portion of a Physical Change may involve loading and verification of the new Managed Component information into the Cisco ROS Configuration Management Database (CMDB). The configuration portion of a Physical Change includes logical configuration changes targeting proper functionality of the Managed Component will.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- Due to a Customer's growing bandwidth needs they submit on RFC to upgrade their IPS 4125 appliance to a IPS 4270 appliance.

### 3.3.2.3 Customer-requested Move - Physical

A Physical Move is a change required to physically move a Managed Component of the Customer's access control infrastructure from one location to another. For a Physical Move, the Customer or a qualified Cisco Partner is responsible for physically moving the component from one location to the next. Cisco is responsible for making the necessary changes in the Cisco ROS CMDB and the configuration of the Managed Component so that management can continue in the new physical location. The Cisco SOC will work with the Customer to coordinate the Physical Move and re-establish remote management connectivity to the Managed Component.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer is shutting down a hub site and is shifting all security assets to the headquarters site.

### 3.3.2.4 Customer-requested Add - Physical

A Physical Add is the addition of new Managed Component(s) entitled under the Cisco Security Intrusion Prevention Remote Management Service. A data-gathering process involving verification and loading of all Managed Component information in the Cisco ROS CMDB including serial numbers, maintenance contract information, circuit information, Carrier information, and more (as needed).

The Managed Component configuration process includes logical configuration changes to ensure that the new Managed Component can be properly managed.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer is adding a Intrusion Prevention System (IPS) appliance external to their firewall and would like Cisco ROS to manage it for them.

### 3.3.2.5 Customer-requested Add – Logical

Logical Adds include installation of new software on Managed Components of the Customer's intrusion prevention infrastructure to enhance or introduce new services or functionality. Logical Adds do not require a high degree of planning and implications for other Managed Components. If the additional functionality introduces new services to other Managed Components or end users, or if the functionality requires extensive planning, the Logical Add may be treated as a Project and thus incur additional fees billed at the Cisco ROS professional services rate.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The customer is requesting a non-critical software upgrade

### 3.3.2.6 Customer-requested Delete – Logical

Logical Deletes refer to removing a Managed Component from the Cisco Security Intrusion Prevention Remote Management Service so that it is no longer a Managed Component. The Managed Component may or may not still exist in the Customer's network.

A Logical Delete requiring a Cisco security engineer to make modifications to the Customer's intrusion prevention infrastructure to allow the Managed Component to be removed (such as transferring functionality to another Managed Component, modifying access control lists, routing, etc.) will be considered a Project if the Cisco SOC Change Manager determines the work required will exceed 4 hours of engineering time.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to eliminate one of their Intrusion Prevention System (IPS) appliances and transfer the monitoring of a network segment to an existing managed IPS module running multiple contexts (note: This example would also require that the Customer submit an RFC for a Logical Add to configure the additional IPS context on the existing managed IPS module)

### 3.3.2.7 Customer-requested Delete – Physical

A Physical Delete requires a Cisco SOC security engineer to make modifications to the Customer's network infrastructure to allow the Managed Component to be physically removed or replaced by another Managed or Non-Managed Component on the Customer's network (i.e., transferring functionality from one Managed Component to another Managed or Non-Managed Component). Any transfer of functionality from a Managed Component to a Non-Managed Component will be the primary responsibility of the Customer.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The customer is decommissioning a Intrusion Prevention System (IPS) appliance and shifting to an SSM AIP module in an existing managed ASA (note: this example would require the Customer to submit an RFC to Physically Delete the IPS appliance as well as another RFC for a Physical Add for the SSM AIP module)

### 3.3.2.8 Customer-requested Projects

Customer-requested Changes that have one or more of the following attributes typically will be handled as a Project:

- Introduction of a service or functionality that is not currently being used in the Customer's network
- Cisco SOC engineering work required to support the request exceeds four hours
- Significant planning is required before implementation of the change request
- Logical Change involves changes to multiple Managed Components at the same time

**Activities:**

- Cisco SOC Change Manager will assess the scope of the project, coordinate the Cisco ROS CAB, and build out a Statement of Work (SOW) to present to the Customer for acceptance or rejection (as Professional Services fees will normally apply)
- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

**Example:**

- The Customer would like a Cisco ROS SOC engineer to engage on a 10 hour project to help design their intrusion prevention infrastructure using Cisco IPS modules and appliances for a new company that they recently acquired.

**3.3.3 Executing changes**

After changes are executed, the Cisco SOC will notify the Customer that the change has been executed. Once the Customer accepts the change, the Ticket will be closed. The status of changes can be viewed on the Portal.

**Activities:**

- Maintain a ticket history of changes visible through the Portal
- Evaluate change requests
- Authorize and schedule change requests
- Coordinate changes
- Update Portal Tickets to include change status
- Review and close change requests

**Deliverable(s):**

- Executed change
- Portal Ticket updated with change notes

#### 4 Cisco Security Virtual Private Network (VPN) Remote Management Service

The objective of the Cisco Security Virtual Private Network (VPN) Remote Management Service is to manage and monitor the identified security components of the Customer's virtual private network (VPN) infrastructure, targeting availability and security of the Managed Components as the primary areas of focus of this service.

The following Managed Components are covered under the Cisco Security Virtual Private Network (VPN) Remote Management Service:

- Managed Components within Customer's VPN infrastructure as outlined in the Cisco ROS Supported Device List located at [www.cisco.com/go/servicedescriptions/](http://www.cisco.com/go/servicedescriptions/)
- Management Termination router (as needed, Cisco-provided depending on method of remote management connectivity to the Managed Components of the Customer's VPN infrastructure)

##### 4.1 Incident Management for Cisco Security Virtual Private Network (VPN) Remote Management Service

Incident Management is the process used by the Cisco SOC to identify Incidents and restore service or remediate declared incidents as quickly as possible and may involve implementing temporary work-arounds. The Cisco Security Operations Center (Cisco SOC) will proactively monitor for key events and thresholds on Managed Components in the Customer's VPN infrastructure. In the case of undetected events, Customers may declare an Incident by contacting the Cisco ROS Service Desk, communicating via telephone any high priority Incidents (system down, degraded performance, etc.). Low priority incidents should be reported to the Cisco ROS Service Desk via the Cisco ROS Web Portal.

Upon automatic detection or manual submission of an Incident to the Cisco ROS Service Desk, an Incident Ticket is created. The Cisco ROS Service Desk will coordinate with the Cisco SOC during the lifespan of the declared Incident. The Cisco ROS Service Desk is ultimately responsible for coordinating the management of the Incident which includes communicating with the Customer throughout the Incident management process. This communication also includes notification to the Customer that the Incident has been resolved or remediated.

##### 4.1.1 Incident Detection

Cisco monitoring system indicates a fault condition, a performance threshold was exceeded, or a security event has triggered a security Incident.

Activities:

- Monitor (24x7x365) manageable elements of the Customer's network security infrastructure
- Perform ongoing Fault and Performance incident monitoring (re: alerting) on the entitled Managed Components of the Customer's network security infrastructure
- Perform ongoing Security incident monitoring (re: alerting) on the entitled Managed Components of the Customer's network security infrastructure
- Detect Incidents
- Correlate Incidents where applicable

Deliverable(s):

- Confirmed Incidents logged in the Cisco ROS Configuration Management Database (CMDB)

##### 4.1.2 Incident Record

Cisco ticketing system captures alarm / event / correlation data, enriches with relevant Configuration Item (CI) information and creates incident ticket

Activities:

- Enrich alarm information with relevant Configuration Item (CI) information from the Cisco ROS CMDB

Deliverable(s):

- Create Incident Ticket
- Post Incident Ticket online via the Portal for the Customer to view all ticket handling activities and milestones

#### **4.1.3 Incident Communication (E-notification)**

Cisco will electronically notify (E-notify) designated Customer contacts for new Incidents or milestones achieved during the Incident Management process. E-notifications are sent to any email address or email-capable mobile device and will include the Incident Ticket number. The Customer (or its preferred vendor) can always view Incident status and detailed information via the Cisco ROS Web Portal.

Automated electronic notification (E-notification) to specific Customer contact(s) based on Customer's notification requirements as agreed on during the Service Activation process.

Activities:

- Match customer's notification profile with Incident Ticket milestones

Deliverable(s):

- Perform E-notification of Incident Tickets per Customer's notification profile
- Log E-notification records in the Incident Ticket

#### **4.1.4 Incident Priority and Classification**

Incidents will be managed according to the Severity level as determined by IT Infrastructure Library (ITIL) service support framework. Incident Severity level depends on a variety of factors including pre-defined Incident Ticketing attributes such as business impact, urgency and asset value (if applicable and entered into Cisco's Configuration Management Database during the Service Activation phase). Incident Severity level will determine the Incident Priority level set by the Cisco SOC on a per-incident basis.

Activities:

- Evaluate Incident Severity and prioritize all Incidents into Priority 1 (P1), Priority 2 (P2) and Priority 3 (P3) Incident categories
- Classify Incidents into Fault, Performance or Security Incident categories

Deliverable(s):

- Properly prioritized Incidents based on Incident Ticketing attributes
- Report status prioritized Incident against its associated Service Level Objectives (SLO) as defined in the Service Level Management (SLM) section of this document

#### **4.1.5 Incident Investigation and Diagnosis**

Cisco SOC engineers utilize Incident Remediation procedures to collect any additional data required to fully diagnose and match the Incident to a known error in the Cisco ROS Knowledge Base (KB). Cisco SOC engineers will work to quickly isolate the root cause of the Incident. Once root cause isolation has occurred, Cisco SOC engineers will update the Incident Ticket with information related to root cause isolation and then proceed to the Incident resolution and restoration phase.

Activities:

- Collect additional data to properly diagnose root cause of the Incident
- Attempt to match Incident to a known error in the Cisco ROS Knowledge Base (KB)

## Deliverable(s):

- Update Incident Ticket with root cause isolation information for Fault and Performance Incidents
- Update Incident Ticket with root cause security event information for Security Incidents
- Perform E-notification for this Incident Ticket event milestone (if requested by the Customer)

**4.1.6 Incident Resolution and Restoration**

Cisco SOC engineers utilize Incident Remediation procedures and work to restore services within agreed service levels, initiating any Requests for Change (RFCs) as needed for restoration.

After the Incident has been isolated down to its root cause, Cisco SOC engineers will work to resolve the Incident. Resolution is complete when functionality is restored to the affected Managed Component(s) or, in the case of a Security Incident, a recommendation is made to the Customer to remediate the Incident. The resolution process includes any action the Cisco SOC requires to restore functionality to a Managed Component or remediate a Security Incident on the Customer's network infrastructure.

The Cisco SOC will utilize work-around solutions to restore all or partial functionality when full functionality cannot be restored within committed timeframes as defined in the Service Level Management section of this document. When a work-around is utilized, the Incident will continue to remain open and will be worked by Cisco SOC engineers until resolved, in accordance with the priority level of the Incident.

Incident resolution and restoration may include Cisco SOC security engineers working directly with the Customer's network IT team to resolve fault and performance incidents on the entitled Managed Components or to assist with the remediation of security incidents detected on the customer's network infrastructure. Cisco SOC security engineers may provide recommendations for remediation of an infected host (if detected). The Customer is ultimately responsible for any patching of infected hosts on their network.

Should the Cisco SOC require a configuration change in a Managed Component to resolve an issue or implement a work-around, the Cisco SOC will follow the Change Management Process established with the Customer

## Activities:

- Resolve Fault and Performance Incidents on Managed Components
- Remediate Security Incidents on the Customer's network infrastructure
- Submit, when needed, a Cisco-recommended Request For Change (RFC) in accordance with the Change Management Process established with the Customer to tune benign traffic or implement a temporary work-around
- Dispatch third party vendors, as needed and appropriate, within the resolution steps prescribed by the Cisco SOC and in accordance with the Cisco SMARTnet or Cisco Services for IPS service terms on the affected Managed Components. As vendors are dispatched, the Incident Ticket will be updated with information related to the dispatch
- Update Incident Ticket to include notes detailing Fault and Performance Incident resolution or recommendations for remediating Security Incidents
- Perform E-notification for this Incident Ticket milestones, if requested by the Customer

## Deliverable(s):

- Updated Incident Ticket with resolution details on Faults and Performance related Incidents
- Updated Incident Ticket with recommendations detailing how to remediate a malicious Security Incident
- Updated Incident Ticket with justification for classifying benign Security Incidents
- Cisco-recommended Request for Change (RFC) for tuning a recurring benign Security Incident as determined by Cisco SOC engineers

#### 4.1.6.1 Incident Escalations

Escalation driven by elapsed time against SLOs ensuring effective routing of Incidents to appropriate technical resources as required. A Customer may request escalation of a Incident Ticket at any time via the Portal or Telephone telephone call to the Cisco ROS Service Desk. The Cisco SOC will refer Incidents to the Customer as needed and escalate the Incident with the Customer within the Customer's escalation guidelines until the Incident is resolved (ie: fault and performance incidents) or remediated (ie: security incidents).

Activities:

- Ensure Incident is being handled by appropriate Cisco SOC engineering resources to meet SLOs
- Escalate Incident as appropriate in the Cisco SOC or with the Customer per the established escalation procedures

Deliverable(s):

- Updated Incident Ticket to include escalation notes
- Incidents resolved or remediated in accordance with SLO targets
- Perform E-notification for this Incident Ticket event milestone, if requested by the Customer

#### 4.1.7 Incident Closure

Once the Cisco SOC declares an Incident resolved and verified, the incident will be closed. In the event that the Incident reoccurs, a new Incident Ticket will be created to accurately reflect the recurring nature of the Incident and aid in the identification of Problems. Depending on frequency, recurring Incidents may trigger the reactive Problem Management process which may include a Cisco-recommended Request For Change (RFC) to resolve the recurring Incident.

Any authorized Customer agent may also proactively request Incident Ticket closure via the Portal or Telephone. The Cisco SOC will review the request and work in conjunction with the Cisco ROS Service Desk to close the Incident Ticket or follow up with the Customer for more information as needed.

Activities:

- Confirm Incident is resolved
- If Incident reoccurs, depending on frequency and attributes of the Incident, open a Cisco-recommended RFC to resolve recurring Incident

Deliverable(s):

- Update Incident Ticket to include closing notes
- Close the Incident Ticket
- Perform E-notification for this Incident Ticket event milestone, if requested by the Customer.

### 4.2 Problem Management for Cisco Security Virtual Private Network (VPN) Remote Management Service

The goal of Problem Management is to minimize the adverse impact of Incidents resulting from errors in the Customer's network by delivering a systematic approach for diagnosing the root causes of Incidents and preventing their reoccurrence by recommending the elimination of the underlying errors whenever possible. To achieve this goal, Cisco SOC engineers will diagnose the root cause of Incidents and then initiate actions to improve or correct the situation.

#### 4.2.1 Reactive Problem Management

Reactive problem management describes the problem management processes that primarily support incident management. These processes are initiated when an incident cannot be matched to a known error. A problem is declared for the purpose of tracking the activities that lead to identifying a root cause and a resolution to the incident's underlying error. The process concludes when a known error, including its root cause and resolution, has been identified and recorded in the known error database. The known error will then be used to resolve and close all associated open and future incidents.

## Activities:

- Utilize Problem Management procedures to collect additional data required to analyze the root cause
- Utilize error data, technical expertise, and product and development resources to isolate a root cause for the error
- Document recommended remediation and resolution procedures, and assist Incident Management team in the resolution of an error
- Error is closed and handed back to the Incident Management team for any further Incident Management activity

## Deliverable(s):

- Faster Incident resolution for repetitive Incidents
- Accurate and updated known error database

## Example:

- A Customer's network may be infected with a virus that is causing latency issues on the VPN network and disrupting the Customer's business. While the Cisco SOC Incident Management team implements a work-around for the Customer a Problem Management security engineer researches the issue, identifies the virus, isolates the root cause and logs their findings in the Cisco ROS known error database. If and when a similar Incident is raised on the Customer network, the Cisco ROS SOC will be able to leverage the known error database to quickly resolve the Incident.

**4.2.2 Proactive Problem Management**

Proactive Problem Management prevents the occurrence or limits the adverse impact of future incidents. The Cisco SOC will analyze Incident trends to identify patterns and systemic conditions. In the event a trend is detected, the results will be introduced into the Problem Management process. The Cisco SOC analyzes different data sets based upon a variety of triggers that would indicate that a Managed Component should be further evaluated. Not all the aforementioned triggers are necessarily indicative of a problem requiring resolution.

## Activities:

- Identify recurring Incidents and refer to Incident Management for resolution
- Analyze trends for Incidents on Managed Components
- Monitor the resolution
- Document applicable error, remediation, recovery, and resolution information in the Knowledge Base

## Deliverables:

- Reduce the number of errors in the Customer's network

## Example:

- Cisco SOC Problem Management engineer performs a configuration review of a Customer's VPN router and delivers a actionable list of recommendations to the Customer to tighten up the access policy on the router

**4.3 Change Management for Cisco Security Virtual Private Network (VPN) Remote Management Service**

Change Management is the process used by the Cisco SOC to apply standardized methods and procedures for authorizing, documenting, and performing all changes. The objective of Change Management is to make necessary Cisco-recommended and Customer-requested changes in an efficient and accountable manner, utilizing standard processes.

**4.3.1 Change Origination**

The first step in initiating the Change Management process is the origination of a Request for Change (RFC). RFCs may originate from two categories: Cisco-recommended changes and Customer-requested changes. Both changes are summarized in the tables below.

<b>Cisco-Recommended Changes<sup>1</sup></b>		
<b>Changes Required To:</b>	<b>Typically resulting in:</b>	
Resolve an Incident or implement a work-around for an Incident	Logical or physical change	
Respond to a critical vulnerability or threat	Logical change	
Apply a software update to a entitled Managed Component	Logical change	
Resolve a known error identified during the Problem Management process	Logical or physical change	
<b>Customer-Requested Changes</b>		
<b>Changes Required To:</b>	<b>Category</b>	<b>Change description</b>
Add, Delete or Change physical component on existing Managed Component	Change	Physical change
Change existing logical functionality (Upgrades)	Change	Logical change
Physically move a Managed Component	Move	Physical move
Add a new Managed Component	Add	Physical add
Addition of new functionality <sup>2</sup>	Add	Logical add
Remove an existing Managed Component	Delete	Physical delete

<sup>1</sup> There will be no additional charges for any Cisco-Recommended changes

<sup>2</sup> Any Customer-requested Logical Change that results in the activation of additional functionality on a Managed Component will be evaluated on a case-by-case basis and discussed with the Customer. If Cisco determines that the additional functionality will increase service support requirements in the Cisco SOC the Customer may be asked to incur additional recurring monthly charges for Cisco SOC support of the additional functionality.

Activities:

- A Change Ticket is initiated by Cisco or the Customer
- The Change Ticket is categorized as described in the table above
- The Customer tracks the progress of the change throughout its lifecycle

Deliverable(s):

- Creation of a Change Ticket on the Cisco Portal for the Customer to view

#### **4.3.1.1 Cisco-Recommended Changes**

Cisco-recommended changes originate from the Cisco SOC. Before executing a Cisco-recommended change, the Cisco SOC will evaluate the change and make a recommendation to the Customer that will include details regarding the criticality and timeframe for implementation of the change. The Cisco SOC will not execute a change until the Customer has authorized or pre-authorized the change to be made.

Activities:

- Communicate the criticality and timeframe associated to the change

- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket

#### 4.3.1.1.1 Cisco-recommended Changes required to resolve an Incident

During the course of the Incident management process, the Cisco SOC may decide to make changes to Managed Components in order to resolve Incidents. These changes are typically logical changes to access control Managed Component configurations for the purpose of troubleshooting and implementing temporary workarounds, and can also include changes to enable troubleshooting issues with third party vendors.

Changes required to resolve Incidents are implemented as needed by the Cisco SOC in accordance with agreed upon Change Management processes established with the Customer.

Activities:

- Logical configuration changes to implement a temporary work-around or aid in troubleshooting an Incident during the Incident Management process including logging level changes
- Logical configuration changes to apply software updates during the Incident Management process or the normal service support activities associated the Service and the entitled Managed Components
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket

#### 4.3.1.1.2 Cisco-recommended Changes to respond to a critical Vulnerability or Threat

Cisco recognizes that certain critical vulnerabilities have the capability to degrade a Customer's system and severely limit network services. As new vulnerabilities are released or threats become known, the Cisco SOC will evaluate the severity and potential impact to the entitled managed component(s) of the Customer's access control infrastructure. If the vulnerability or threat is judged by the Cisco SOC to be critical with respect to Customer safeguards, or the Customer is impacted by the vulnerability, the Cisco SOC will recommend changes to correct the issue and/or mitigate the threat. If requested by the Customer, changes will be executed according to the priorities and terms contained in Customer-Requested Change section of this service description.

Changes to address critical vulnerabilities will be performed at the earliest possible time, in coordination with Customer and the agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to respond to a critical vulnerability or threat identified by the Cisco SOC
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process including updating all activities in the Change Ticket

#### 4.3.1.1.3 Cisco-recommended Changes to address known errors uncovered during the Problem Management process

During the course of the Problem Management process, the Cisco SOC may recommend changes to the Managed Components of the Customer's access control infrastructure in order to resolve a known error.

Changes required to resolve known errors are implemented as needed by the Cisco SOC in accordance with agreed upon Change Management processes established between Cisco and the Customer.

Activities:

- Logical configuration changes to resolve a known error identified during the Problem Management process
- Communicate the criticality and timeframe associated to the change
- Obtain approval for executing the change
- Follow established Change Management process.

#### 4.3.2 Customer-Requested Changes

Customer-requested changes are changes that originate with the Customer. The Customer can use the Cisco Portal to submit Customer-requested changes. This will automatically initiate the Change Management process. The Customer can also call the Cisco ROS Service Desk and describe the change request over the phone. The Cisco ROS Service Desk will make the initial evaluation of the Request For Change (RFC) and coordinate with the Cisco SOC Change Manager in compliance with the agreed upon Change Management process established between Cisco and the Customer.

A Change Management process that includes costs, timeframes, and guidelines for the work to be completed is based on the classifications of the RFC and governs all Customer-requested changes. These guidelines ensure that the Cisco SOC receives proper notice (re: lead time) to arrange the required resources to complete the work in an expeditious manner. The specifics of the Change Management Process, including any additional costs, are outlined and reviewed with the Customer during the Service Activation phase.

The Cisco SOC Change Manager evaluates the potential impact of Customer-requested changes and will determine if a Cisco security engineer will need to discuss the implications of a requested change with the Customer. If the Cisco SOC Change Manager determines that the change requires additional information, planning, diligence or testing, the Cisco SOC Change Manager will coordinate the Cisco SOC Change Advisory Board (CAB) which may, in their discretion, refuse the Customer-requested change if they determine that the change will adversely affect the functionality of the entitled Managed Components or the security posture of the Customer's access control infrastructure. The Cisco SOC Change Manager will have responsibility for communicating acceptance or rejection of the Request for Change (RFC).

Activities:

- Cisco ROS Service Desk makes initial evaluation of the RFC and coordinates with the Cisco SOC Change Manager
- Cisco SOC Change Manager classifies the change into one of the following categories: Move, Add, Change, Delete or Project
- Cisco SOC Change Manager coordinates with the Cisco SOC Change Advisory Board (CAB) as needed to determine the level-of-effort and business risk associated to the change request as defined in the IT Infrastructure Library (ITIL) Change Management framework under the following change categories: Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or a designated member of the Cisco SOC CAB communicates with the Customer regarding the criticality and timeframe associated to the change in accordance with the change attributes
- Cisco SOC Change Manager obtains approval from the Customer for executing the change
- Cisco SOC follows the established Change Management process including updating all activities in the Change Ticket

##### 4.3.2.1 Customer-requested Change - Logical

A Logical Change includes changes to software on Managed Components of the Customer's access control infrastructure. Logical Changes requiring an increased level of planning, involving multiple Managed Components or requiring more than four hours of work will typically be treated as a Project. The Cisco SOC Change Manager will have the responsibility of determining the level-of-effort to support the Logical Change request and if it should be treated as a Project.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to allow active FTP connectivity through a managed VPN router.

#### 4.3.2.2 Customer-requested Change - Physical

A Physical Change is a change to a hardware element on an existing Managed Component such as a network module. The installation portion of a Physical Change may involve loading and verification of the new Managed Component information into the Cisco ROS Configuration Management Database (CMDB). The configuration portion of a Physical Change includes logical configuration changes targeting proper functionality of the Managed Component.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to add a network interface card (NIC) to their existing managed router

#### 4.3.2.3 Customer-requested Move - Physical

A Physical Move is a change required to physically move a Managed Component of the Customer's access control infrastructure from one location to another. For a Physical Move, the Customer or a qualified Cisco Partner is responsible for physically moving the component from one location to the next. Cisco is responsible for making the necessary changes in the Cisco ROS CMDB and the configuration of the Managed Component to ensure that management can continue in the new physical location. The Cisco SOC will work with the Customer to coordinate the Physical Move and re-establish remote management connectivity to the Managed Component.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to ensure that a managed router is brought back under Cisco SOC management once the device is physically moved and plugged back in at a new physical location

#### 4.3.2.4 Customer-requested Add - Physical

A Physical Add is the addition of new Managed Component(s) entitled under the Cisco Security Virtual Private Network (VPN) Remote Management Service. A data-gathering process involving verification and loading of all Managed Component information in the Cisco ROS CMDB including serial numbers, maintenance contract information, circuit information, Carrier information, and more (as needed).

The Managed Component configuration process includes logical configuration changes to ensure that the new Managed Component can be properly managed.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to add a router on to their VPN infrastructure to enable connectivity from a remote site to their headquarter location

#### 4.3.2.5 Customer-requested Add – Logical

Logical Adds include installation of new software on Managed Components of the Customer's VPN infrastructure to enhance or introduce new services or functionality. Logical Adds do not require a high degree of planning and implications for other Managed Components. If the additional functionality introduces new services to other Managed Components or end users, or if the functionality requires extensive planning, the Logical Add may be treated as a Project and thus incur additional fees billed at the Cisco ROS professional services rate.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to enable the Firewall Feature set on a managed router

#### 4.3.2.6 Customer-requested Delete – Logical

Logical Deletes refer to removing a Managed Component from the Cisco Security Virtual Private Network (VPN) Remote Management Service so that it is no longer a Managed Component. The Managed Component may or may not still exist in the Customer's network.

A Logical Delete requiring a Cisco SOC security engineer to make modifications to the Customer's VPN infrastructure to allow the Managed Component to be removed (such as transferring functionality to another Managed Component, modifying access control lists, routing, etc.) will be considered a Project if the Cisco SOC Change Manager determines the work required will exceed 4 hours of engineering time.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to terminate the Cisco Security Virtual Private Network (VPN) Remote Management Service on a managed router. The router will remain on the Customer's network.

#### 4.3.2.7 Customer-requested Delete – Physical

A Physical Delete requires a Cisco SOC security engineer to make modifications to the Customer's network infrastructure to allow the Managed Component to be physically removed or replaced by another Managed or Non-Managed Component on the Customer's network (i.e., transferring functionality from one Managed Component to another Managed or Non-Managed Component). Any transfer of functionality from a Managed Component to a Non-Managed Component will be the primary responsibility of the Customer.

Activities:

- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC to decommission a VPN router at a remote site and transfer VPN connectivity for that site to another VPN termination device at that same location.

#### 4.3.2.8 Customer-requested Projects

Customer-requested Changes that have one or more of the following attributes typically will be handled as a Project:

- Introduction of a service or functionality that is not currently being used in the Customer's network
- Cisco SOC engineering work required to support the request exceeds four hours
- Significant planning is required before implementation of the change request
- Logical Change involves changes to multiple Managed Components at the same time

Activities:

- Cisco SOC Change Manager will assess the scope of the project, coordinate the Cisco ROS CAB, and build out a Statement of Work (SOW) to present to the Customer for acceptance or rejection (as Professional Services fees will normally apply)
- Cisco SOC Change Manager evaluates the Customer's Request For Change (RFC) and categorizes the RFC into Standard, Minor, Significant, Major or Urgent
- Cisco SOC Change Manager or Change Assignee coordinates with the Customer according to the Change Management process established with the Customer

Example:

- The Customer submits an RFC for a Cisco Internetwork Operating System (Cisco IOS) upgrade involving 20 VPN routers in order to take advantage of new key functionality in the upgraded version of Cisco IOS

#### 4.3.3 Executing changes

After changes are executed, the Cisco SOC will notify the Customer that the change has been executed. Once the Customer accepts the change, the Ticket will be closed. The status of changes can be viewed on the Portal.

Activities:

- Maintain a ticket history of changes visible through the Portal
- Evaluate change requests
- Authorize and schedule change requests
- Coordinate changes
- Update Portal Tickets to include change status
- Review and close change requests

Deliverable(s):

- Executed change
- Portal Ticket updated with change notes

## 5 Service Level Management for Cisco Security Remote Management Services

### 5.1 Change Category Service Pricing and Scheduling for Customer-Requested RFCs

Customer-Requested RFCs<sup>1</sup>

Category	Type	Turnaround Time <sup>3</sup>	Standard Fees per Managed Component	Notes	Expedite Fees <sup>6</sup>
Change	Logical <sup>2</sup>	24 Hours	\$0	Urgent Logical Changes will be handled on a case-by-case basis and may not include any expedite fees if resources are available in the Cisco SOC.	\$200 per request
	Physical	7 Days	\$350		\$1200 + Time and Materials / per device <sup>4</sup>
Move	Physical	14 Days	\$350		
Add	Physical	14 Days	\$350		
	Logical	14 Days	\$350		
Delete	Logical	7 Days	\$0		
	Physical	14 Days	\$0		
Project	Any change requiring greater than four hours of work	See Note <sup>5</sup>	Cisco Security Remote Management Professional Services rate: \$250 per hour with 4 hour minimum	Scope and cost to be determined on a case-by-case basis and handled within the Cisco ROS Statement of Work (SOW) process	\$1000 minimum (depends on project size)

<sup>1</sup> All changes will be handled by the Cisco SOC Change Manager based on the IT Infrastructure Library (ITIL) framework definitions of changes including: Standard, Minor, Significant, Major and Urgent changes. All changes determined to be Standard changes are pre-approved changes and may or may not require execution during the Customer's change management maintenance window. All Urgent changes will be evaluated on a case-by-case basis and the Customer may incur Expedite Fees depending on Cisco SOC resource availability at the time of the Urgent change request.

<sup>2</sup> The Cisco SOC Change Manager will monitor the total volume of all Logical changes on a 30-day rolling period. If the Cisco SOC Change Manager determines that the total service support hours for handling the Customer's Logical Change requests exceeds 20 hours in any given 30-day rolling period, the Cisco SOC Change Manager will convene a meeting with the Cisco SOC CAB to build out a Statement of Work (SOW) billed at the Cisco ROS Professional Services rate of \$250 per hour to accommodate any Logical Change work in excess of 20 hours per month.

<sup>3</sup> Unless otherwise stated all timeframes are in calendar days

<sup>4</sup> Timing subject to hardware, vendor, and / or Cisco SOC resource availability to execute the change

<sup>5</sup> Addition of a new managed site usually requires PDI (Plan, Design, and Implement) work that must be handled by a qualified PDI Security Partner prior to activating any Cisco Security Remote Management Services on any Managed Components.

<sup>6</sup> "Expedite Fee" means charges paid by the Customer to Cisco to perform Customer-requested changes without providing Cisco with the required lead-time stated by change category / type in the table above. Also, as stated in note 1, the Customer may incur expedite fees for Cisco SOC engineers to handle any Urgent change requests (i.e., in an emergency type of situation). The Cisco SOC Change Manager will make every effort to coordinate Cisco SOC engineering resources as quickly as possible to avoid

**Customer-Requested RFCs<sup>1</sup>**

Category	Type	Turnaround Time <sup>3</sup>	Standard Fees per Managed Component	Notes	Expedite Fees <sup>6</sup>
----------	------	------------------------------	-------------------------------------	-------	----------------------------

expedite fees. Expedited Customer-requested changes can always be cancelled or changed; however, the Customer will still be responsible for half of the expedite fee if the Urgent change request is not cancelled within 24 hours of the scheduled change.

## 5.2 Management Reporting and Web Portal for Cisco Security Remote Management Services

Cisco provides an online Portal for the Customer to review Tickets, Ticket metrics, and reports for all Managed Components of Cisco Security Remote Management Services.

### Deliverable(s):

- Portal logins for each of the Customers authorized employees
- Inventory information on the Portal (as available per Managed Component) including:
  - System description
  - Maintenance vendor
  - Maintenance coverage type and contract number
  - Serial number
  - IP Address
- Incident and Service Request Ticket information on the Portal (as available) including:
  - Incident and Service Request Ticket identification number – The tracking number assigned by the Cisco SOC to each Ticket.
  - Incident and Service Request Ticket opened date and time – The date the Ticket was opened
  - Incident and Service Request Ticket description – A brief description of the Incident(s) or Service Request(s) detailed in the Ticket
  - Incident and Service Request Ticket status – The current status of the Ticket as determined by the most recent note entered in to the ticket
  - Site(s) affected – Within the Ticket, the site locations where Managed Components are affected
- Reports on the Portal (as available per Managed Component or for entitled service including):
  - Performance Analysis – data analysis reports that graph utilization and performance metrics on Managed Components (as available depending on Managed Component)
  - Exceptions – data analysis reports that graph high and low exceptions for utilization and errors on Managed Components (as available depending on Managed Component)
  - Security Event Response Time -- shows the elapsed time between the declaration of a Security Incident and the subsequent classification of that Security Incident (as recorded in the Cisco ROS Incident Management Ticketing System)
  - Fault Event Response Time -- shows the elapsed time between the declaration of a Fault or Performance Incident and the subsequent Isolation of that Fault or Performance Incident (as recorded in the Cisco ROS Incident Management Ticketing System)

- Security Event Rate of Occurrence -- shows the number of Security Incidents categorized into each malicious security classification (i.e., Attack, Probable Attack, Successful Attack, Worm, Virus, Recon) that was handled by the Cisco SOC during the given time period
- Daily Threat Exposure -- shows a normalized aggregate total impact of all detected malicious Security Incidents handled by the Cisco SOC during a particular day
- Monthly Threat Exposure -- shows a normalized aggregate total impact of all detected malicious Security Incidents handled by the Cisco SOC during a particular month
- Top 10 Types of Attacks -- shows the most frequently triggered IPS signatures and firewall syslog pneumonics that led to Security Incident declaration during the given time period
- Top 10 Attacked Hosts -- shows the most frequent targets of detected Security Incidents handled by the Cisco SOC during the given time period
- Top 10 Sources of Attack -- shows the most frequent sources of attack for detected Security Incidents handled by the Cisco SOC during the given time period
- PIX Audit Log -- tracks the activity occurring on a specific Cisco PIX firewall and shows the audit log activities generated by a specific PIX device during the given time period

<b>Incident Management Service Level Objectives (SLOs) for Cisco Security Remote Management Services<sup>1</sup></b>				
<b>Key Performance Indicator (KPI)</b>	<b>KPI Details</b>	<b>Cisco Security Access Control Remote Management Service</b>	<b>Cisco Security Intrusion Prevention Remote Management Service</b>	<b>Cisco Security Virtual Private Network (VPN) Remote Management Service</b>
MTTN	Notify Customer of Fault, Performance or Security Incidents within X minutes	15 min	15 min	15 min
MTTInv	Investigate Fault & Performance Incidents within X minutes	30 min	30 min	30 min
MTTBa	Begin Analysis of Security Incidents within X minutes	30 min	30 min	n/a
MTTCa	Complete Analysis and Provide Recommendations for Remediating Security Incidents within X minutes	75 min	75 min	n/a
MTTIso	Isolate Root Cause of Fault & Performance Incidents within X minutes	75 min	75 min	75 min
MTTR <sup>5</sup>	Resolve Fault & Performance Incidents within X hours	P1: 4 hours <sup>2</sup> P2: 24 hours <sup>3</sup> P3: 72 hours <sup>4</sup>	P1: 4 hours <sup>2</sup> P2: 24 hours <sup>3</sup> P3: 72 hours <sup>4</sup>	P1: 4 hours <sup>2</sup> P2: 24 hours <sup>3</sup> P3: 72 hours <sup>4</sup>

<sup>1</sup> Cisco will use commercially reasonable efforts to meet the Service Level Objectives (SLOs) set forth in this table. The SLOs will not apply if unavailability of the Managed Services is caused by Customer's content that is added to the Managed Component application software, bugs in custom code deployed on Managed Components, failed upgrades or enhancements on Managed Components, acts of Customer or its agents, network unavailability outside the Cisco ROS network, dedicated remote network connectivity outages, or events beyond Cisco's control.

<sup>2</sup> Priority 1 Incidents on an entitled Managed Component where the Managed Component is unavailable and severely disrupting / impacting the Customer's business. Cisco and the Customer will commit any necessary resources 24x7 until the Incident is resolved / remediated

<sup>3</sup> Priority 2 Incidents on an entitled Managed Component where the Managed Component is unavailable or its functionality is severely degraded and Customer's business is moderately disrupted. Cisco and the Customer will commit full-time resources during normal business hours Monday through Friday to resolve / remediate the Incident

<sup>4</sup> Priority 3 Incidents on an entitled Managed Component where the Managed Component is unavailable or its functionality is moderately degraded and Customer's business is minimally disrupted. Cisco and the Customer are willing to commit resources as available during normal business hours to resolve / remediate the Incident and restore service to satisfactory levels.

<sup>5</sup> For Incidents requiring a third party field dispatch (i.e., replacement of a Managed Component or restoration of a internet circuit), regardless of Incident priority, Cisco provides no specific Mean Time To Resolve (MTTR) target as the MTTR will depend heavily on underpinning contracts with the dispatched third party. The Cisco ROS SOC shall use all commercially reasonable efforts to restore service as quickly as possible and work with the dispatched field technician to drive an issue to resolution, including

working in accordance with the Managed Component maintenance contract (if known) as well as any Service Level Agreements (SLAs) the Customer has negotiated with any dispatched party or other vendor (if known and recorded as a Configuration Item (CI) in the Cisco ROS Configuration Management Database (CMDB)). For any Incidents requiring Return Materials Authorization (RMA) activity on a Managed Component with a current Cisco maintenance contract (i.e., SmartNet, Cisco Services for IPS, etc), the MTTR target will be set as close as possible to the maintenance contract terms and conditions on the Managed Component, taking into consideration the Priority level of the Incident.

### **5.3 Service Reviews**

For entitled Customers, the Cisco SOC will conduct recurring Service Reviews (monthly and/or quarterly) to review the current management reporting data available for Cisco Security Remote Management Services. Only those Customer's that have purchased all three services under Cisco Security Remote Management Services (which include Cisco Security Access Control Remote Management Service, Cisco Security Intrusion Prevention Remote Management Service and Cisco Security Virtual Private Network (VPN) Remote Management Service) will be entitled to receive this recurring Service Review conducted by the Cisco SOC security team.

## **6 Customer Responsibilities for Cisco Security Remote Management Services**

### **6.1 Service Activation**

To ensure that Cisco is enabled to provide Cisco Security Remote Management Services for Managed Components, Cisco requires the Customer to:

- Assign a project manager to represent the Customer during the service activation phase
- Assign a technical lead that will assist Cisco with establishing the network access required for remote management.
- Supply all required information contained in the Service Activation Kit (SAK) provided during the Service Activation phase.

### **6.2 Connectivity and Network Access**

- The Managed Component where the Remote Network Management Channel terminates on the Customer premise must provide access to all other Managed Components. The Customer will allow logical network access to the other Managed Components via the Managed Component that the management channel is terminated on
- Cisco Security Remote Management Services are delivered using specific ports and protocols. The Customer will open up the required ports and protocols to enable Cisco to collect the data for all Managed Components covered under Cisco Security Remote Management Services
- To ensure that the Cisco SOC can provide Cisco Security Remote Management Services, the Cisco SOC requires the Customer to provide Cisco SOC with full read/write access using network management protocols that included enabling full administrative privileges (enable mode, root access, admin access, etc.) to all Managed Components entitled under Cisco Security Remote Management Services.

### **6.3 Operations Support**

- A Customer contact will be assigned for each Managed Component for which Cisco Security Remote Management Services have been purchased to assist Cisco with technical and non-technical troubleshooting and administrative tasks as normal course of action for delivering the entitled Service.
- Customer is responsible for assigning a Process Manager that will review and coordinate the approval of changes to the Cisco Operations Support Manual.

### **6.4 Managed Components**

- The Customer is responsible for providing and maintaining the network equipment outside of the Managed Components scope
- The Customer is responsible for the physical security of the Managed Components
- The Customer must agree to allow Cisco to retain and publish aggregate statistics and metrics for non-identifiable trending analysis

- The Customer is responsible for providing back-up procedures and configuration data for the network equipment (non-Managed Components)

### 6.5 Support for Non-Managed Components

- Cisco does not provide any support for Non-Managed Components. Cisco has a professional Services process for handling support requests. Contact a Cisco ROS Service Account Manager (SAM) for details on the Cisco ROS Individual Case Basis (ICB) process
- The Customer is responsible for managing Non-Managed Components

### 6.6 Communications and Change Management

- Cisco takes a co-management approach to Cisco Security Remote Management Services allowing the Customer and other Customer-approved vendors to retain access to Customer's managed components. Because multiple parties may be able to make changes to the managed and non-managed components of the Customer's network, Cisco SOC requires that anyone with access to the Customer's network environment follow a consistent and documented Change Management Process. This process will be reviewed and agreed upon prior to completion of the Service Activation phase
- The Customer is responsible for updating the Cisco SOC with current data with respect to the Customer information as well as all Managed Components, as needed, via the Portal
- The Customer is responsible for the timely delivery of information required for configuration of Managed Components and Customer information (including notification procedures)
- The Customer should notify the Cisco ROS Service Desk 72 hours in advance of any scheduled maintenance windows
- The Customer maintains sole responsibility for informing Cisco of Customer employee status changes
- The Customer is responsible for providing and maintaining a list of Customer employees authorized to request changes
- The Customer is responsible for providing and maintaining an escalation path within the Customer's employee base
- The Customer is responsible for end-user training of the Cisco ROS Portal. Service Requests for training can be submitted via telephone or the Portal

## 7 Remote Management Activation for Cisco Security Remote Management Services

The Remote Management Activation is a process in which Cisco prepares the Customers IT infrastructure for Cisco management. Using our proven Service Activation methodology enables an efficient and low-impact effort of enabling the Customers IT infrastructure to receive Cisco's management Services. This framework includes:

- Discovering the managed components on the Customer's IT infrastructure
- Planning the transition to management
- Implementing management operations

### 7.1 Discovering the IT Infrastructure

Discovering the IT infrastructure includes the pre-implementation activities that provide Cisco with a high-level understanding of the Customers business and IT infrastructure needs. This assists our team in having an accurate understanding of the Customer's requirements before the planning and implementation processes begin.

Activities:

- Identify key Customer participants and setup initial kick-off meeting
- Have initial engagement with the Customer

Deliverable(s):

- Introduction package

Cisco will work with Customer to discover and get an understanding of the infrastructure. In this case, the purpose of planning the transition of Remote Management Activation is to prepare both the Customer and the Cisco SOC for a smooth management transition. This process involves collecting and validating all technical details required to enable remote IT infrastructure management, ensuring the Customer has a clear understanding of service features, and establishing joint interaction methods. Each Managed Component will be assessed to ensure that no further work is needed before remote management begins.

## 7.2 Planning the Transition to Remote Management Activation

The purpose of planning the transition is to prepare both the Customer and Cisco for a smooth management transition. This process involves collecting and validating all technical details required to enable remote IT infrastructure management, ensuring that the Customer has a clear understanding of Service features, and establishing joint interaction methods. Each site will be assessed to ensure that no further work is needed before the managed components located at the physical site are brought under management.

**Activities:**

- Establish key relationships with the Customer
- Work with the Customer to develop an implementation plan
- Gather relevant site information from the Customer and/or Cisco or Partner PDI Team via the Service Activation Kit (SAK)
- Gather the key Managed Component information from the Customer and/or Cisco or Partner PDI Team via the Service Activation Kit (SAK)
- Enter the Customers Managed Component information into the Cisco ROS Configuration Management Database (CMDB)
- Define an escalation plan for the Cisco SOC and the Customer
- Align on the Change Management Process
- Complete applicable Letters of Agency (LOA)
- Order the remote network management circuit (if applicable and necessary)
- Configure, ship and deliver the Cisco ROS remote network management channel termination router (if applicable and necessary)

Deliverable(s):

- Completed Service Activation Kit (SAK)
- Completed Cisco Operations Support Manual
- Letter of Agency (LOA) on file in the Cisco ROS database
- Cisco Transition Plan document
- Installation date for network management circuit (Cisco provided)

### 7.2.1 Remote-Infrastructure Operations Readiness Approval

Prior to implementing remote management operations, the Cisco ROS SOC will either approve an existing managed device or make recommendations required for accepting a new managed infrastructure. If the necessary changes are not made, acceptance of the order may be delayed or withdrawn. If the Customer wishes to engage Cisco to implement the recommendations, a separate Agreement to make the changes may be required.

### 7.3 Implementing Management Operations

Implementing management operations involves executing the transition project plan developed in the planning the transition to management process. To provide a single point of contact to apply ongoing focus on established timelines and commitments, Cisco will appoint a designated project coordinator.

During this phase, Cisco will establish management connectivity and ensure the Customer contacts are aware of how to interact with the Cisco SOC during delivery of services.

Activities:

- Cisco SOC will be providing remote network management connectivity and a associated management router (if applicable and necessary) to a single (US domestic preferred) Customer location end-point to effectively manage the network security infrastructure components
- Cisco will install a Cisco remote network management channel termination router (if applicable and necessary)
- Establish management access for each Managed Component via the Cisco-provided Management circuit (VPN or Frame)
- Review the configuration of all Managed Components to ensure readiness for remote management
- Work with the Customer on any initial management configuration issues and/or changes required for successful management
- Begin ongoing Incident monitoring of Managed Components

Deliverable(s):

- Establish Cisco ROS Portal access and verify Managed Components inventory
- Publish scheduled events via notes in the master Service Activation Ticket viewable on the Portal
- Train Customer employees on how to use the Portal
- Provide the Customer with a complete inventory of Managed Components, published on the Portal
- Remote network management channel termination router(s) configured, shipped and installed on customer premise (if applicable and necessary)
- Management Connectivity installed and verified
- Perform gap analysis between Managed Components inventory and what is on the original Purchase Order, resolving any discrepancies
- Email the Customer a copy of the Cisco Operations Support Manual

As necessary, for the Cisco SOC to perform its responsibilities as stated in this Service Description, the Cisco SOC will maintain an information repository of data in the Cisco ROS CMDB with respect to the Customer and the Managed Components that will be referenced in the Cisco Operations Support Manual.

### 8 Services Not Covered

In addition to those "Services Not Covered" posted at [www.cisco.com/go/servicedescriptions/](http://www.cisco.com/go/servicedescriptions/) , the following are not supported under the Cisco Security Remote Management Services:

- Support of a product (including a Managed Component) that is not on the Cisco ROS Supported Device List, unless otherwise authorized via the Cisco ROS Individual Case Basis (ICB) process. For details regarding the ICB process please contact a ROS Service Account Manager (SAM).

-END-