Service Description: Cisco Security Remote Management Services

Technology Addendum to Cisco Remote Management Services Common Service Description

This document referred to as a Technology Addendum describes the Cisco Security Remote Management Services.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/ : (1) Cisco Remote Management Services RMS Common Service Description ("RMS Common Service Description"); (2) Glossary of Terms; (3) List of Services Not Covered.

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. If not already covered in your MSA or equivalent services agreement, this document should be read in conjunction with the Related Documents identified above. 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/servicedescriptions/.

Service Summary

Cisco Security Remote Management Services and other optional services are intended to supplement a current support agreement for Cisco products, and only available where all the Managed Security Components in a Customer's network are supported through a minimum of core services such as Cisco's SMARTnet and Software Subscription Services, as applicable. Cisco shall provide the 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 Security Remote Management Service

The Service described below will act as additional or clarifying definition to detail contained within the RMS Common Service Description.

Cisco Security Remote Management Services provides remote network security monitoring and management support for security components and devices within the Customer's security infrastructure.

This Appendix describes the services capabilities, supported devices, elective changes, and reports delivered with Cisco Remote Management Services for Security. The primary distinction between the Managed security service as compared to the Monitoring service is the addition of proactive security analysis and remediation of event traffic by Cisco's Security Operations Center personnel. This addition provides Customers with the 24/7 event analysis, proactive and reactive configuration changes as well as device tuning. The services support all of the primary Cisco Security technologies; A list of all supported devices is included in Section 2.4.

1. Service Levels

The Cisco Security Remote Management Service is offered in two service levels, Monitoring and Managed.

Activities for the Cisco Security Remote Management Service not covered in the Cisco RMS Common Remote Service Description are described in this Technology Addendum.

- The Monitoring Service level provides monitoring, correlation, and reporting of your security devices and infrastructure.
- The Managed Services level provides the addition of security event analysis, advanced security reporting, event classifications mitigations and remediation
- Optional Services can be provided on an "As-needed" basis under separate Purchase Orders.

1.1. Service Level Activities

In addition to what is described in the Common Remote Management Services Common Service Description, The Security Monitoring and Managed Service levels and Optional services include:

Table 1 Monitoring, Managed Services and Optional Services Summary

Activities / Deliverables		Monitoring Service	Managed Service	Optional Services	Required Optional Services
Management Readiness Assessment		✓	✓		
Incident Management	Incident Management is an ITIL process used by Cisco RMS to identify Incidents, restore service and remediate declared incidents as quickly as possible and may involve implementing temporary work-arounds. RMS will proactively monitor for key events and thresholds on managed components in the Customer's network infrastructure. In the case of undetected events, Customers may declare an Incident by contacting the Cisco RMS Service Desk, communicating via telephone any high priority Incidents (system down, degraded performance, etc.). Low priority incidents should be reported to the Cisco RMS Service Desk via the Cisco RMS Web Portal. Upon automatic detection or manual submission of an Incident to the Cisco RMS Service Desk, an Incident Ticket is created. The Cisco RMS Service Desk will coordinate with the Cisco CE during the lifespan of the declared Incident. The Cisco RMS 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.	✓	✓		

Device Monitoring		✓	✓		
Incident Record	Enrich alarm information with relevant IntelliShield information from the Cisco IntelliShield Deliverable(s):	✓	✓		
Incident Notification		✓	✓		
Incident Priority and Classification			✓		
Incident Investigation and Diagnosis	Security events will be root caused to one of the following: Attack, Successful Attack, Probable Attack, Reconnaissance, Misuse, Worm, Virus, or Benign		✓		
Incident Resolution and Restoration			✓		
Incident Escalations			✓		
Incident Closure			✓		
Advanced Security Event Correlation	Advanced Security Event Correlation - Identifies patterns based on multi-dimensional correlated data that delivers visibility by tying together parent and children related performance and failure problem activities across the network.	✓	✓		
Incident Resolution			✓		
Root Cause Analysis Reports				✓	Customer Engineer Level I
Ticket Trending and Analysis				✓	Customer Engineer Level II Option
Review / Assess Cisco Field Notices				✓	Customer Engineer Level II Option
Web Accessible Portal		✓	✓		
Standard Reports		✓	✓		
Advanced Reports			✓		
Custom Reporting				✓	Operations Manager Level II
Operations Manager Level I and II				✓	
Customer Engineer Level I and II				✓	
Defined Changes				✓	Elective Changes
Custom Scoped Changes				✓	Elective Changes
Regulatory Compliance Management				✓	Compliance Management Package
Configuration Policy Management				✓	Compliance Management Package
Software Image Management (SWIM)				✓	Compliance Management Package

2. Security Reporting

The Cisco Management Application Platform ("MAP") collects and gathers log and security event information from the Managed Security Components covered within the service. This information is compiled and made available via reports available on the Services portal. Device level reports available are listed below. Detailed information on all reports can be found at: http://www.cisco.com/en/US/products/ps6192/serv_datasheets_list.html

2.1. Standard Reports

Standard Security Reporting	Report Description
CPU and Memory Reporting	CPU utilization (%) memory pool utilization (%), memory pool free, memory pool largest free
Network Interface Reporting	Interface utilization (%) bandwidth usage, errors and discards
TCP/IP Port Monitoring	TCP/IP port availability reporting
IPSEC Statistics	Active tunnels, Total inbound authentication failures, total authentications, total packets received/dropped
Failover Status	Hardware information and status
Availability Reporting	System availability
Inspection Load	Indicates how much traffic inspection capacity the sensor is using
Missed Packet Percentage	Average of missed packet inspection
Partition Utilization	% of space allocated to each partition

2.2. Advanced Reports

Advanced Security Reports	Report Description
Intrusion Prevention Blocked Attack Report Summary A summary of suspected attacks in which the IPS sensor or enforcement point blocked a specific packet and/or connection, including signature fired, category, severity, and src/dst addresses.	
Top Blocked Attacks by Signature	A ranking of top fired signatures that resulted in a blocked attack
Top Blocked Attacks per Sensor	A ranking of top blocked attacks by IPS Sensor
Top Source Blocked Attacks	A ranking of the top Source IP address that was blocked
Top Destination Blocked Attacks	A ranking of the top destination IP address that was blocked
IPS Signature Categories	A ranking of the top fired signatures that resulted in a block by category
Intrusion Prevention Summary Reports	
Top Fired Signatures / Signature severity	A ranking of the signatures fired most often and the severities of those signatures by severity
Top Attacker Source	A ranking of the top Source IP address that resulted in a signature to alarm
Top Attacked Destinations	A ranking of the top destination IP address that resulted in a signature to alarm
Signature Severity Summary by Sensor	High, medium, and low severities per Intrusion Prevention Device A ranking by individual sensor of the top signatures triggered by severity
Top Fired Signatures Severity	Cumulative totals (high, medium, low) of IPS Signature severities triggered across the entire intrusion prevention environment
Firewall Summary Report A summary of the connections and traffic that have been denied or permitted as a result of the applied firewall policy or access control list.	
Total Denied Packets	A ranking by firewall of the total denied attempts
Top Denied Source Addresses	A ranking by top source IP address which resulted in a denied attempt by a firewall policy
Top Denied Destination Address	A ranking by top destination IP address which resulted in denied attempt by a firewall policy

Top Denied Protocols	A ranking by top protocols which resulted in a denied attempt by a firewall policy
Top Denies by Access Control Policy	A ranking by Access Control List of the most utilized polices which resulted in a denied attempt
Authentication Failure Summary Reports A summary of failed authentication attempts	
Top Source Address Failed Attempts	A ranking of the top source IP addresses which resulted in failed login attempt
Top Destination Address Failed Authentication Attempts	A ranking of the top destination IP addresses which resulted in a failed login attempt
Top Authentication Failures by Device	A ranking by device of the top failed login attempts
Top Username Failed Attempts	A ranking by Username of the top failed login attempts
Bandwidth Summary Reports	
Top Applications	Presents the top applications across the environment in terms of bandwidth usage
Top Source / Destination	Presents Top bandwidth consumers by source address and destination address

2.2.1. Security Event Rate Report

This report is also provided as part of the Advanced Reporting functionality.

The security event rate report provides detailed event classifications of each security incident from the Intrusion Prevention System (IPS). The classifications include the following:

- **Exploits** - Identifies alarms or traffic that contains an actual exploit to a vulnerability
- **Successful Compromise** – Identifies alarms or traffic that have successfully exploited a known vulnerability
- **Denial Of Service** – Identifies alarms or traffic that is targeted at a specific set of devices or networks with the intent of causing the system or network to become unresponsive to legitimate requests
- **Malware/Virus/Trojan/Worm** – Identifies alarms or traffic associated with malicious intent to compromise the integrity of a system or networks, obtain sensitive data or information and/or propagate malicious software with the intent of infecting other systems and networks.
- **Authentication/Access/Authorization** – Identifies alarms or traffic that attempt to improperly gain access or administrative privileges to a system or networks
- **Reconnaissance Attempts** – Identifies alarms or traffic patterns which discover and gather network information, host identification, vulnerabilities and open ports.
- **Misuse** – identifies alarms that are in violation of corporate network policies; example, IRC, gaming, and torrent
- **Fault –** Identifies alarms associated with device availability status including processes and connectivity
- **Suspicious Traffic** - Identifies alarms considered suspicious either due to their unusual nature or due to the presence of only limited information

2.3. Custom Reports

Provides for the ability to create or modify the types of reports based upon the available data. Each request for Custom Reporting must be evaluated and mutually agreed upon between Cisco and the Customer. Operations Manager Level 2 is a pre-requisite for Custom Reporting.

3. Cisco Security RMS Supported Devices

Supported Devices

- Cisco Intrusion Prevention Systems
- Cisco Adaptive Security Systems (ASA)
- Cisco ISR Series Routers IOS Intrusion Prevention System
- Cisco ISR Series Routers IOS Firewall
- Cisco Firewall Services Module
- Cisco ISR Series and ASA VPN
- Cisco IronPort Email Security Appliances
- Identity Services Engine (ISE)

Supported non-Cisco Devices

- TippingPoint
- IBM/ISS
- Checkpoint
- Juniper

Services provided by Cisco include the monitoring of foundation and security elements associated with security functionality.

Aggregate event traffic in excess of 2000 events/second may require additional Cisco Management Application Platform (MAP) capacity upgrade

Full details and product lists for Managed Components can be found at:
http://www.cisco.com/en/US/products/ps6192/serv_datasheets_list.html

4. Customer Requested Change Management

Customers purchase a block of support hours that can be leveraged across all Defined Changes Categories and Custom Scoped Elective Changes that a Customer has under their RMS contract. The Customer must have a sufficient balance of support hours on account to cover the requested change. Additional support hours may be purchased if required.

4.1. Defined Changes

Defined Changes are categorized into Small, Medium, and Large activities. A Defined Change is a requested change by the Customer. Defined Changes are not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the needed type of change and submits a Defined Change Request on the Portal.

Customers purchase Support Hours that can be leveraged across all Defines and Customer Scoped Change Categories that a Customer has under their RMS contract. The Customer must have a sufficient balance of Support Hours on account to cover the requested change. Additional Support Hours may be purchased if required.

Small Defined Changes (Type 1)

- Standard Access Control List (ACL) policy update
- Basic Network Address Translation (NAT) change or security device policy
- Single IPS signature basic tuning
- Adding of Access Control List (ACL) or policy

Medium Defined Changes (Type 4)

- Enabling and testing new feature or security functionality
- Multi-line firewall Access Control List (ACL) change and testing that spans multiple managed devices
- Detailed policy creation, Access Control List (ACL), or Network Address Translation (NAT)
- Advanced IPS tuning request
- Virtual Private Network (VPN) addition for remote device

Large Defined Changes (Type 8)

- Large scale changes that impact multiple devices and
- Network address re-designs and network security policy changes
- Disaster recovery and failover testing for multiple sites and network security devices
- IPS rebuilds
- Creation of new virtual sensor
- Advanced security feature implementation, tuning and testing

4.2. Custom Scoped Changes

Custom Scoped Changes are Customer requested changes that fall outside Incident and Problem (Standard) changes for restoring service and requires custom scoping through an SOW. Custom Scoped changes will require a mutually agreed upon statement of work (SOW). See RMS Common Service Description for more details of Custom Scoped Change support. An example of a Custom Scoped Change activity is listed below.

- Implementation and testing of new security features across multiple devices