MANAGED FIREWALL SERVICES - SERVICE GUIDE V.2

Last Modification Date: 09/09/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1 MANAGED SERVICES OVERVIEW

Managed Network and Monitoring Services provides organizations with the management and monitoring of their network infrastructure, to improve availability, whether the infrastructure is on premises, a third-party datacenter or the cloud. This Service Guide describes Managed Network Services in general (part one) and then describes the specific details of the managed network devices for which this service guide is intended (part two). This document clarifies the scope of the service, service level, roles and responsibilities, and other specifications of the service for customers of this service. This document may get updated from time to time to add additional clarification and details related to this service.

1.1 MANAGED SERVICES - GENERAL SERVICE DETAILS

In Scope

- This Managed Service offers management and monitoring of devices and software according to this Service Guide and the InterVision Work Order to aid in resuming normal operations. Additional requests above and beyond will be based upon time and material expense to the Customer.
- Detection, isolation, diagnosis of each fault and restoration to normal operating conditions, testing and documenting each fault within the InterVision trouble ticket system
- Ownership of resolution of the problem on behalf of the Customer and act as an agent for the Customer under executed letters of agency
- Notify the Customer of the progress of all faults per Customer provided contact process.
- Critical software and firmware updates to resolve issues. Premium service level offers periodic updates as detailed later in this service guide.
- Summary reports delivered via our monitoring portal to help the Customer understand traffic, clients, and application usage
- Assistance with warranty replacement and vendor escalations.
- Premium service level assists with changes to individual devices. Mass additions/deletions or changes (greater than 5) are not covered via the Managed Network Services agreement and will be considered project billable tasks.
- Premium Service level offers bi-annual reviews to identify significant business impacting risks. This review includes identification of software updates, end of life, end of support, device performance, and critical configuration errors.
- Safeguard customer's proprietary information using commercially reasonable efforts to securely access client network through an encrypted tunnel.

Out of Scope

- Hardware or Software installation or non-RMA replacement is not included with network support unless specifically stated below. Professional services may be engaged to assist with installation, upgrade or replacement.
- Software license and subscriptions are not included. Management devices and software provided as part of the Managed Service will be licensed.
- Netflow reporting is available as an additional optional paid service. The device to be covered by Netflow must support the application and have the necessary capabilities to provide reporting appropriate to need.
- Mass configuration changes to covered devices that are required, due to Customer upstream or downstream projects, are not covered as part of the service.
- Coverage for devices not under agreement are ineligible for support of any type.

Customer Requirements

To allow for successful monitoring and management of devices and execution of SLAs, Customer responsibilities include:

- Providing all network and device information for the InterVision Managed Services team and tools to discover the contracted devices and enable monitoring. This information includes network diagrams, site information, circuit information and Customer Vendors, Letters of Agency, and current software levels.
- Providing computing resources to run InterVision's monitoring and collection tools, and the means for the Collector to contact the InterVision Data Center.
- Performing configuration of devices and network, as necessary, to facilitate monitoring and management of the contracted devices. In the event the customer is unable or does not have the personnel to enable monitoring and management of devices, InterVision's Professional Services can be engaged for assistance at an incremental cost.
- Provide devices access - Remote access to devices must be available for support. The client is responsible for out of band access, along with in-band access.
- Provide a distribution list of Customer contacts to receive alarm triggered notifications and reports
- Supply InterVision team with all the necessary security information including dial-in numbers, access ID's, passwords, SNMP community names necessary for InterVision to perform the Services
- Provide notification contact and escalation lists for use by InterVision during business and non-business hours.
- Provide InterVision team with site contact to facilitate access to equipment and connection terminations, along with out-of-hours access procedures
- Notify InterVision within 72 hours of any changes to the contracted devices via a service/change ticket.
- Execute letters of agency notifying vendors, such as carriers, that InterVision will represent the Customer by isolating and troubleshooting Customer's network problems
- All devices and applications must have vendor support contracts and operate at currently supported vendor versions.
- All devices must be in a supportable state, including current versions of software supported by vendor, with all critical patches applied, in a production capable state with no known failures or functions in order to be covered. Remediation efforts to bring software to current version including patches to make a device production capable will be billable to the customer.

1.2 SERVICE LEVELS

- Monitoring Service provides 24/7 monitoring and customer notification. Notification includes automated alerts as well as notification via service personal to client for critical events. This does not include trouble shooting and device support. Support is available for changes to monitoring settings and assistance with reports.
- Essential Service offers 24/7/365 phone and ticket support. it does not include dispatch for onsite support.
- Essential Service with Dispatch offers 24/7/365 phone and ticket support. It includes dispatch for onsite support[1, 2] where remote support is unable to fulfill eligible service events such as RMA device replacement.
- Premium Service offers 24/7/365 phone and ticket support. It includes dispatch for onsite support[1, 2] where remote support is unable to fulfill eligible service events such as RMA device replacement. Premium Service includes addition services including extended coverage for changes, devices software upgrades, periodic health and performance reviews and life-cycle management.

[1] *Applies to devices covered under Managed Network Services in the continental US. International onsite coverage may be added via a custom scope of work.*
[2] *Onsite support is at the discretion of InterVision as determined necessary*

1.3 SUPPORT

Service	Monitor Only	Essential	Premium

Event notification	Included	Included	Included
Phone & Ticket Support 24 hours, 7 days a week	Included for monitoring issues	Included, with SLA	Included, with SLA
Onsite Support **	Not Included	Not Included, No SLA.	Included, with SLA

* All coverage times are based on the local time zone of the supported device.
** Applies to devices covered under Managed Services in the continental US. International onsite coverage may be added via a custom scope of work.

- If an outage or network problem occurs which is determined to be a site related issue InterVision managed service team will document the Incident within its ticketing system. Examples of site related Incidents are: Loss of power to site, damage to premise cabling, accidental disconnection of site cabling or Equipment.
- For Routers, SD-WAN and Firewalls, if an outage or network problem occurs which is determined to be a Broadband Carrier circuit failure, InterVision will, via a Letter of Agency from Customer, contact the relevant Carrier or ISP and report the Incident for resolution. InterVision will then continue to manage the problem and follow up with the Carrier or ISP to ensure service is restored as quickly as possible. This service is included unless specified in the service SKU description as not included.
- If an outage or network problem occurs which is determined to be a failure of CPE, InterVision will diagnose and attempt to resolve the issue remotely. If the outage cannot be resolved remotely, InterVision will escalate to the Customer and/or technician dispatch when needed. Determination of the necessity of on-site services is at the sole discretion of InterVision, If dispatch is requested and cancelled within 48 hours of requested dispatch time, a $500 cancellation fee will be applied.

1.4 SERVICE ACTIVATION

InterVision employs a structured process to help ensure a smooth transition to Managed Infrastructure and Monitoring services. Our Project Management Office (PMO) owns the process with the Onboarding Engineer (OE), holding the ultimate responsibility and serving as the single point of contact (SPOC).

Steps to activate service

1. Data gathering

1. Customer service manual
2. Order form

- Monitoring collector/ Support workstation Deployment and Configuration
- Onboard customer devices
- Add data from step one into systems
- Finalize customer onboarding
- Send any found issues with onboarding for client to review
- Go Live/ Customer training
- Perform true up / Project Closeout

Network Infrastructure Evaluation

For new client environment onboarding not recently set up by InterVision Services, an evaluation is required that will review the environment to ensure it is in a supportable state. Software and Firmware will be reviewed to be current or within one major software version behind current. This evaluation will also review configuration, access control policies for critical risks. Software/Firmware, configuration and access control issues and risks must address to be in a supportable state. Environment updates may be identified as requiring additional project time to

address and InterVision reserves the right to modify SLAs or refuse service if Environments are not current and critical risks addressed.

2 SERVICE SPECIFICATION - MANAGED FIREWALL SERVICE

The Managed Firewall Service covers the designated Firewalls and provides availability/performance monitoring, support and specified management of the covered devices that are part of a network that is designed to block unauthorized access while permitting outward communication. For a list of currently supported devices, please contact your account representative.

This managed service is based upon each instance of a firewall (physical or virtual).

- This is a managed service for client-owned equipment.
- As the number of firewalls increase fees for this service will increase
- Managed Firewall Management Console service is required if firewalls are centrally managed
- This service is available in multiple service tiers which includes: 1) Essential; 2) Essential with Dispatch; 3) Premium.
- Essential – this tier offers 24/7 monitoring, incident resources, issue remediation, vendor escalations, RMA assistance and critical patching to resolve issues. .
- Essential with Dispatch – This tier includes all the capability of the Essential service and adds the ability to provide remote hands service at your site to assist with device replacements and other issues requiring skilled remote hands to resolve.
- Premium - This tier builds upon the previous tiers and adds change management, health and performance reviews, access control and policy reviews, periodic software and firmware updates and life-cycle notifications.
- This service includes support of the firewall devices, the SW subscriptions directly associated with the firewall (including VPN, IDS/IPS, URL filtering, network malware protection), and a single attached circuit (if specified in the Service Order). This service can also include support the firewall management console.

2.1 SERVICE DETAILS - MANAGED FIREWALL SERVICE

This service picks up day-to-day monitoring and management of the firewall in production. Design and installation service may be obtained via our Professional services. Benefits of this service include:

- Support Desk with 24/7/365 coverage
- Ongoing monitoring, incident response, and troubleshooting performed by our knowledgeable InterVision network and security managed services staff.
- Execution of changes to resolve issues
- Assist your organization in establishing usage controls to support your business needs
- Patching to resolve issues***/****
- Summary reports delivered via the monitoring portal to help you understand traffic, clients, and application usage**
- Assistance with warranty replacement and vendor escalations***
- Circuit vendor escalations to resolve issues if specified in the service item description

Premium service level also includes the following:

- Devices changes including changes to ACLs, firewall rules, advance security policies, ports, VLAN and VPN and other configuration items. For Mass (greater than 5) additions/deletions or changes are not covered via the Service and will be considered project billable tasks
- Scheduled software and firmware updates are provided with the Premium service level.
- 6-month proactive firewall review to include performance monitoring, capacity analysis, life cycle management, firewall rule cleanup, remote access VPN software upgrade and firewall upgrade

- Specific to Meraki MX, InterVision is unable to take on the management of Meraki devices that require 2-factor authentication into the Meraki console.

* Additional services that can be provided with incremental fees.

** Full troubleshooting may require coverage and managed support of all upstream network components.

***InterVision Managed Firewall Services is not a replacement for vendor support coverage. Without vendor support coverage the operations center cannot perform critical vulnerability patching or upgrades.

****HA devices require that both active and passive devices must be covered to provide both monitoring and alerting, and patch management services.

2.2 ROLES AND RESPONSIBILITIES MATRIX

Managed Firewall Service Responsibility Matrix		InterVision Support	
Description	**Customer**	**Essential Support**	**Premium Support**
Initial Device Installation and Configuration			
Firewall licensing and maintenance contracts	X		
Initial design and configuration of Firewall, WAN/LAN	X*		
Physical or virtual Firewall install	X*		
Switch Port or VLAN Configuration	X*		
Create new firewall rules	X*		
Create new authentication methods	X*		
Create new remote access VPN (IPSEC/SSL)	X*		
Create and implement high availability features****	X*		
Create Access Control Lists (ACL)	X*		
* InterVision professional services can be provided to assist with this responsibility.			
Onboarding	**Customer**	**Essential Support**	**Premium Support**

Provide Firewall information (account, password, location, MAC address,…)	X		
Provide Customer Escalation information	X		
Vendor support contracts	X		
Firewall Onboarding (Configuring of SNMP, Syslog, SSH and Backups)	Client to configure for essential		X
One-time Audit of the Firewall for configuration issues, vulnerabilities, and risks. (prior to support activation; may find issues that require remediation)			X
Setup Monitoring and Logging		X	X
Update monitoring thresholds per client requirements		X	X
Manage Notification Profiles		X	X
Monitoring and alerting	**Customer**	**Essential Support**	**Premium Support**
Firewall Monitoring and Alerting - Essential		X	X
Firewall Monitoring and Alerting - Premium		*	X
*Alert only, no response services (see monitoring table below)			
Incident and Problem Management	**Customer**	**Essential Support**	**Premium Support**
Internet Circuit vendor escalations (if purchased with circuit support)		X	X
Vendor escalations (Open issue tickets with vendor for supported service areas)		X	X
Process RMA from Vendor		X	X

Replacement of device from RMA (Remote configuration migration to new device (if compatible with config backup and access to the device))		X	X
Replacement of device from RMA (ONSITE)		*	X
Firewall Incident Management Remediation		X	X
Troubleshoot availability issues and down Firewall		X	X
Troubleshoot NAT and port forwarding rules			X
Troubleshoot remote access VPN (IPSEC/SSL)			X
Troubleshoot site to site VPN			X
Troubleshoot access control lists (ACL)			X
Troubleshoot IDS/IPS module			X
Troubleshoot web-filtering integration (ScanSafe, WebSense, WCCP)			X
Troubleshoot Firewall integration			X
Root cause analysis			X
Other Firewall Incident manage			X
			*Requires onsite dispatch option to be added

Change Management	**Customer**	**Essential Support**	**Premium Support**
Administer user access	X		
Administer device accounts		X	X
Log and Store change information		X	X
Backup prior to change		X	X

Review of changes prior to making the change		X	X
Modify high availability features			X
Create or modify ACL rules			X
Create or modify URL filtering /IPS/IDS rules			X
Modify remote access VPN policy (IPSEC/SSL)			X
Administer device accounts			X
Create or modify Site to Site VPN			X
Create new remote access VPN policy			X
Implement / setup 3rd party integrations	X*		
Modify 3rd party integrations			X
* InterVision professional services can be provided to assist with this responsibility.			
Patch Management	**Customer**	**Essential Support**	**Premium Support**
Firmware updates to resolve service impacting issues		X	X
Critical Security Vulnerability patching			X
6-month Proactive firewall version review and upgrade ****			X
6-month proactive remote access VPN upgrade (software provided to customer, requires helpdesk agreement for installation)			X
Firewall Upgrades			X
Proactive Monitoring and Maintenance	**Customer**	**Essential Support**	**Premium Support**

Device Backups (Cisco Devices)		X*	X*
Performance Tuning and Management (Bi-annual review)			X
Capacity Analysis (Bi-annual review)			X
Life Cycle Management Notification (Bi-annual review)			X
Firewall Rule Cleanup (Bi-annual review)			X
*If device only allows one backup target, customer may take on this responsibility.			
Firewall Management Console Management	**Customer**	**Essential Support**	**Premium Support**
Monitor Console for Availability & Performance		X	X
Standard reporting setup per client request			X
Basic dashboard setup per client request			X

2.3 MONITORING

The following monitors will be implement as permitted by the environment.

Essential Monitoring	Trigger Method	Threshold	Severity
Network Device Not Responding	5 pings every 2 minutes	100% packet loss for 5 minutes	10
Network Memory Critical	polled every 3 minutes	90%+ for 10 minutes	9
Critical Network Device Interface Staying Down	SNMP and/or Syslog	Down for 5 minutes	9
Network Device Critical Interface High Utilization	polled every 1 minute	95% for 5 minutes	8
Network Device Failover Detected	Syslog	1 event	8

Network CPU Critical	polled every 3 minutes	90%+ for 10 minutes	7
Network Device Critical Interface Flapping	Syslog	Critical Interface Goes Down and Up 3 times in 15 minutes	7
Network Device Hardware Critical	Syslog	1 event	6
Network Critical Interface Error Critical	SNMP polled every 1 minute	Critical Interface showing 5% in or out error rate	6
Premium Monitoring	**Trigger Method**	**Threshold**	**Severity**
ASA Certificate Has Expired	Syslog	1 event	10
ASA Failover Detected	Syslog	1 event	8
ASA Orderly Reload Detected	Syslog	1 event	8
ASA Certificate Due To Expire	Syslog	1 event	6
FMC VPN Status Critical	Syslog	1 Event	10
FMC Classic License Critical	Syslog	1 Event	10
FMC Smart License Critical	Syslog	1 Event	10
FMC ISE Connection Status Critical	Syslog	1 Event	10
FMC User Agent Status Critical	Syslog	1 Event	10
FMC URL Filtering Critical	Syslog	1 Event	10
FMC Cluster Status Critical	Syslog	1 Event	10
FMC Card Reset Critical	Syslog	1 Event	10
FMC Disk Status Critical	Syslog	1 Event	10

FMC Hardware Alarms Critical	Syslog	1 Event	10
FMC Health Monitor Process Critical	Syslog	1 Event	10
FMC Platform Faults Critical	Syslog	1 Event	10
FMC Power Supply Critical	Syslog	1 Event	10
FMC Threat Data Updates on Devices Critical	Syslog	1 Event	8
FMC Smart License Warning	Syslog	1 Event	6
FMC User Agent Status Warning	Syslog	1 Event	6
FMC Threat Data Updates on Devices Warning	Syslog	1 Event	6
FMC ISE Connection Status Warning	Syslog	1 Event	6
FMC URL Filtering Warning	Syslog	1 Event	6
FMC Cluster Status Warning	Syslog	1 Event	6
FMC Card Reset Warning	Syslog	1 Event	6
FMC Disk Status Warning	Syslog	1 Event	6
FMC Hardware Alarms Warning	Syslog	1 Event	6
FMC Health Monitor Process Warning	Syslog	1 Event	6
FMC Platform Faults Warning	Syslog	1 Event	6
FMC Power Supply Warning	Syslog	1 Event	6

FMC Classic License Warning	Syslog	1 Event	6
FMC VPN Status Warning	Syslog	1 Event	6
FortiGate FIPS CC Entered Error Mode	Syslog	1 Event	10
FortiGate CC Entered Error Mode	Syslog	1 Event	10
FortiGate License Has Expired	Syslog	1 Event	10
FortiGate Report Disk Full	Syslog	1 Event	8
FortiGate Log Quota Warning	Syslog	1 Event	8
FortiGate DLP Archive Full	Syslog	1 Event	8
FortiGate Quarantine Disk Full	Syslog	1 Event	8
FortiGate Power Supply Failure	Syslog	1 Event	8
FortiGate IPS Archive Full	Syslog	1 Event	8
FortiGate Exit Bypass Mode	Syslog	1 Event	6
FortiGate License Expiring	Syslog	1 Event	6
FortiGate IP SEC Tunnel Down	Syslog	1 Event	6
FortiGate Log Disk Full	Syslog	1 Event	6
FortiGate HA Sync Failed	Syslog	1 Event	6
FortiGate Enter Bypass Mode	Syslog	1 Event	6

Palo Alto Out Of Memory Condition	Syslog	1 Event	10
Palo Alto Power Supply Failure	Syslog	1 Event	9
Palo Alto System Shutdown Initiated	Syslog	1 Event	8
Palo Alto Link Down	Syslog	1 Event	8
Palo Alto HA Link Down	Syslog	1 Event	8
Palo Alto Seed Out Of Sync	Syslog	1 Event	6
Palo Alto Licensed Feature Expiring	Syslog	1 Event	6

2.4 REPORTING

For all Managed Firewall Services, the following service reports are available provided quarterly.

- Hardware availability
- Device performance and capacity
- Trouble tickets
- Change tickets
- Monthly overview reports
- SLA reports

3 SUPPORT COMMITMENT

3.1 TO ENSURE THAT INCIDENTS ARE REPORTED IN A STANDARD FORMAT, THE FOLLOWING PROBLEM PRIORITY DEFINITIONS WILL BE ADHERED TO.

- Priority 1 (P1)—An existing network or Services are “down” or there is a critical impact to your business operations. Customer and InterVision will commit all necessary resources around the clock to resolve the situation. Proactive monitoring alarms classified as a severity of ‘Service Down’ or ‘Critical’ fall into this category.
- Priority 2 (P2)—Operation of an existing network or Services are severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of covered products. Customer and InterVision will commit full-time resources around the clock to resolve the situation. Proactive monitoring alarms classified as a severity of ‘Trouble’ fall into this category.
- Priority 3 (P3)—Operational performance of the network or Services are impaired while most business operations remain functional. Customer and InterVision will commit resources during normal business

hours to restore service to satisfactory levels. Proactive monitoring alarms classified as a severity of 'Attention' fall into this category.
- Priority 4 (P4)—Operational performance of the network or Services are only minimally impaired while business operations remain functional. Customer and InterVision will commit resources during normal business hours to restore service to satisfactory levels.

Priority 3 and Priority 4 service tickets can be opened via InterVision's portal https://support.hostedcafe.com/cafe For Priority 1 and Priority 2 we recommend calling the operations Center at **1-800-731-7096.**

SLO Metric	Priority 1	Priority 2	Priority 3	Priority 4
Respond	0.3 hours Goal % = 95	0.5 hours Goal % = 95	4.0 hours Goal % = 95	4.0 hours Goal % = 95
Assign	0.5 hours Goal % = 85	4.0 hours Goal % = 85	24 hours Goal % = 85	24 hours Goal % = 85
Resolution	4.0 hours Goal % = 85	24 hours Goal % = 85	48 hours Goal % = 85	5 Days Goal % = 85

3.1.1 TO ENSURE THAT CHANGES ARE REPORTED IN A STANDARD FORMAT, THE FOLLOWING PROBLEM PRIORITY DEFINITIONS WILL BE ADHERED TO:

Change Definition: The addition, modification or removal of any supported service, service component or device that could have an effect on business processes and services. All changes are assigned a risk level, Low, Moderate, High and type, Standard, Urgent, Scheduled, Client Performed.

- Standard Change—A low to moderate risk change, that can be executed with no set date or time. Typically defined as simple and repeatable changes with low to no impact to the business processes or services.
- Urgent Change— A low, moderate or high risk based change with no set date or time and needs to be executed with an abbreviated time frame. Typically these changes have an immediate risk of business impact that needs to addressed as quickly as possible. *
- Scheduled Changes—A low, moderate or high risk based change that has a defined start and end date for execution. May require additional planning and coordination prior to execution. **
- Customer Performed Changes—A change that will be documented and executed by the client. Upon submission the change will be recorded with InterVision for tracking and trap suppression within the defined change window.

* It is recommended that High Risk Changes be moved to Scheduled changes when possible

** Recommended lead time of at least 72hrs in advance of the scheduled date and time for execution

SLO Metric	Standard	Urgent	Scheduled
Respond	0.5 hours Goal % = 95	0.5 hours Goal % = 95	0.5 hours Goal % = 95
Assign	24 hours Goal % = 85	4 hours Goal % = 85	24 hours Goal % = 85
Resolution	48 hours Goal % = 85	24 hours Goal % = 85	7 days Goal % = 85

3.2 MANAGEMENT TOOLS

InterVision utilizes a variety of 3rd party software products to provide services. These tools include IT Service Managed (ITSM), monitoring, log collection, remote access, and other support and diagnostic tools. InterVision is responsible for selection and maintenance of software and tools used to provide service. InterVision uses prevailing industry practices to select, deploy, and operate these tools making all reasonable efforts to do in a secure manner and to not introduce any undue risks.

InterVision constantly evaluates the market for best-in-breed services to provide our customers, and may, at any time, change the software in use. InterVision will be responsible for the installation and maintenance of any InterVision-provided solution. The use of any other non-InterVision provided solutions will be the customer responsibility to manage and monitor.

Requests for a list of InterVision software tools may be obtain via a request through your Client Service Delivery Manager (for clients subscribing to Service management) or via a ticket.

3.3 DEFINITIONS

Dispatch - This refers to the scheduling of remote hands service at your site to assist with device replacements and other issues requiring skilled remote hands to resolve issues.

EOL - End of Life

EOS - End of Support

Essential Service Level - This is an InterVision Managed Service support level that offer monitoring, incident response and issue remediation.

Hosted Cafe' - Hosted Cafe is a name for the InterVision managed services organization and team. It is used to differentiate the services from other services such as professional services or Customer IT operations.

Monitor only- InterVision will place the Customer premise equipment ("CPE") under support and monitoring only service. The Service covers the specific IT infrastructure devices as detailed in an applicable Service Order. There is no phone support or onsite support with this service.

RMA - Return Merchandise Authorization. This refers to like-for-like device replacement under vendor warranty.

Premium Service Level - This is an InterVision Managed Service support level that offer monitoring, incident response, issue remediation, change management and additional life-cycle management capabilities.