MANAGED FIREWALL SERVICES - SERVICE GUIDE

Last Modification Date: 05/13/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

Managed Firewall Service falls under the SLA and description for the InterVision Managed Network Services.

1 MANAGED NETWORK 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 NETWORK 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.
- Summary reports delivered via our monitoring portal to help the Customer understand traffic, clients and application usage
- Assistance with warranty replacement and vendor escalations.
- 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.
- 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 emails 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 LEVEL OFFERS

- 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.
- Standard Service offers 24/7/365 phone and ticket support. it does not include dispatch for onsite support.
- Enhanced 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 is available for SD-WAN devices. See Managed SD-WAN Service description and details for additional details

[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	Standard	Enhanced	Premium
Event notification	Included	Included	Included	Included
Phone & Ticket Support 24 hours, 7 days a week	Included for monitoring issues	Included, with SLA	Included, with SLA	Included, with SLA

Service	Monitor Only	Standard	Enhanced	Premium
Onsite Support 7AM-7PM MON-FRI**	Not Included	Not Included, No SLA.	Included, with SLA	Included, with SLA
Onsite Support Off-Hours**	Not Included	Not Included, No SLA	Included, with SLA	Included, with SLA
Phone Support – Devices Not Covered by NetTend	Not Included	Not Included	Not Included	Not Included
Onsite Support – Devices Not Covered by NetTend	Not Included	Not Included	Not Included	Not Included

* 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.

- In the event that 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.
- In the event that 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.
- In the event that 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 REPORTING

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

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

1.5 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
    a. Customer service manual
    b. Order form
2. Monitoring collector/ Support workstation Deployment and Configuration
3. Onboard customer devices
4. Add data from step one into systems
5. Finalize customer onboarding
6. Send any found issues with onboarding for client to review
7. Go Live/ Customer training
8. Perform true up / Project Closeout

1.6 SERVICE DELIVERY - INCIDENT AND DEVICE IMPACT CLASSIFICATION

The Managed Infrastructure and Monitoring service employs a sophisticated algorithm called the Ticket Enrichment Engine that utilizes the severity of the incident, and the business criticality of the device to determine the appropriate priority levels. Devices such as SD-WAN, routers and firewalls are defaulted to classification as critical devices, and are automatically prioritized higher than other devices. Customers are able to designate other devices as critical, to decrease/increase their prioritization based upon their business impact

Severity 1	No Ticket	
Severity 2	No Ticket	
Severity 3	No Ticket	
Severity 4	Notification Ticket Closed State	
Severity 5	Notification Ticket Closed State	Upgrade Eligible
Severity 6	P3 Ticket	
Severity 7	P3 Ticket	Upgrade Eligible
Severity 8	P2 Ticket	
Severity 9	P2 Ticket	Upgrade Eligible
Severity 10	P1 Ticket	

Emergency (P1 or P2) services require a phone call to create an incident.

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).

- The service is provide in two service levels. 1) basic firewalls (ACL & VPN), and 2) next generation firewalls that include additional security services for IPS, URL filtering, Malware detection, application controls. When ordering this service Next Generation Firewall must be specified to recieved support for advance security services.
- As the number of firewalls increase fees for this service may increase.
- This is a managed service for client-owned equipment.

2.1 SERVICE DETAILS

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:

- Ongoing monitoring, configuration and troubleshooting performed by our knowledgeable network Hosted Cafe' staff
- Assist your organization in establishing usage controls to support your business needs
- Software and firmware updates per your request*
- Support Desk with 24/7/365 coverage
- Summary reports delivered via the monitoring portal to help you understand traffic, clients, and application usage**
- Assistance with warranty replacement and vendor escalations***
- Mass (greater than 5) additions/deletions or changes are not covered via the Service and will be considered project billable tasks
- Specific to Meraki MX, InterVision is unable to take on the management of Meraki devices that require 2-factor authentication into the Meraki console.

*Extended services are optional services that can be provided with incremental fees. These services may be additional managed services or obtained through professional services.

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

***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 in order to provide both monitoring and patching requirements of the service.

Roles and Responsibilities Matrix

	Client	Hosted Cafe'	Extended Services*
General			

	Client	Hosted Cafe'	Extended Services*
Firewall information (account. password, location, MAC address,…)	X		
Firewall SNMP string	X		
Client escalation information	X		
Vendor support contracts	X		
Installation and Configuration			
Initial design and configuration of Firewall, WAN/LAN	X		X
Physical or virtual Firewall install	X		X
Switch Port or VLAN Configuration	X		X
Create new firewall rules	X		X
Create new authentication methods	X		X
Create new remote access VPN (IPSEC/SSL)	X		X
Create and Implement High Availability features	X		X
Create Access Control Lists (ACL)	X		X
Monitoring			
Setup monitoring and logging		X	
Update monitoring thresholds per client requirements		X	
Manage notification profiles		X	
Setup Firewall dashboard in the customer's portal		X	

	Client	Hosted Cafe'	Extended Services*
Firewall reports setup		X	
Incident and Problem Management			
Incident management		X	
Root cause analysis		X	
Vendor management (Escalations, RMA,…)		X	
Troubleshoot down firewall		X	
Troubleshoot site to site VPN		X	
Troubleshoot NAT and port forwarding rules		X	
Troubleshoot remote access VPN (IPSEC/SSL)		X	
Troubleshoot access control lists (ACL)		X	
Troubleshoot IPS Module and SourceFire	X		X
Troubleshoot web-filtering integration (ScanSafe, WebSense, WCCP)	X		X
Patch Management			
Firmware updates (to resolve issues)		X	
Critical Security vulnerability patching (as required)		X	
Software – minor feature releases, non-critical patches	X		X
Change Management			
Create a new site	X		X

	Client	Hosted Cafe'	Extended Services*
Create or Modify site to site VPN tunnel	X		X
Create or Modify ACL rules		X	
Create URL Filtering/IDS/IPS rules		X	
Modify URL filtering/IDS/IPS rules		X	
Modify Remote access VPN (IPSEC/SSL)		X	
Modify high availability features for firewall and routers		X	
Management			
Administer device accounts		X	
Administer user access	X		
Log and store change information		X	
Backup configuration prior to change (Cisco Devices Only)		X	
Review of changes prior to making the change		X	
HW physical replacement - Process RMA with Vendor		X	
Onsite HW replacement	X		X
Remote HW replacement configuration migration to new device (if compatible with config backup and access to the device)		X	
Performance Tuning and Management	X		X
Capacity Analysis	X		X
Life Cycle Management Notification (EOL, EOS)	X		

	Client	Hosted Cafe'	Extended Services*
Reporting			
Standard Reports		X	
Custom Operations Reports			X

2.2 MONITORING

Managed Firewall Services will monitor the following:

Monitor	Trap Frequency	Threshold	Severity
Device Down- Not responding to ICMP Pings (NT)	5 pings every 2 minutes	80% for 240 seconds	10
Network Memory Critical	3- minutes	85%	9
Critical Network Device Interface Staying Down	1-minutes	5 minutes	9
Network CPU Critical (NT)	3- minutes	90% for 600 seconds	7
Critical Interface- High Utilization (NT)	1-minutes	85% for 600 seconds	7
Network Memory Warning	3- minutes	50%-84% for 600 seconds	5
Network Interface Error Critical (NT)	1-minutes	510% for 600 seconds	5
Dropped Pings- Not Responding to ICMP Pings (NT)	5 pings every 2 minutes	100% for 120 seconds	2
Network CPU Warning (NT)	3- minutes	75%-89% for 600 seconds	1

3 REPORTING

Reports may be limited by device capabilities.

4 SERVICE ACTIVATION

See the main managed infrastructure service guide for details on Service Activation.

5 SERVICE DELIVERY

See the main managed infrastructure service guide for details on Service Delivery.