Managed Firewall

Service description

Make businesses ***run better***, ***grow faster*** and ***do more*** for your customers

TABLE OF CONTENTS

1 Introduction

This document describes the Managed Firewall service of Ingram Micro (hereinafter referred to as Ingram Micro).

Through our flexible Managed services we offer you, as an Ingram Micro customer, the ability to choose for the management of your customers' IT environment, or parts of it, through Ingram Micro's Network Operating Center. The Network Operating Center of Ingram Micro offers the same functionality and experience as your own IT management department without you or your client's organization being burdened with knowledge management, resourcing and specific Network Operating Center solutions. The Network Operating Center is staffed by experienced IT professionals and provides pro-active management and remote support.

1.1 MANAGED FIREWALL AT A GLANCE

Managed Firewall is a managed service where Ingram Micro manages the firewall infrastructure. The scope of the service is described in greater detail in this document.

Ingram Micro offers Managed Firewall in two variants;

1. Managed Firewall ***Basic*** - All Ingram Micro standards are deployed at a standard service level. In the “Basic” variant, the network management is carried out with monitor tooling from the vendor.

2. Managed Firewall ***Standard*** - All Ingram Micro standards are deployed at a standard service level. In the “Standard” variant, the network management is carried out with Auvik monitoring software. Auvik is a professional monitoring platform for Enterprise monitoring of network environments, in which much more is monitored than in the “Basic” variant.

The Managed Firewall service description is based on the following components:

- Supported functions
- Hardware
- Monitoring & Response
- Patch & Release Management
- Backup & Restore
- Service Levels & Reporting

2 Managed Firewall

This chapter describes the purpose and functionality of the different elements that compose Ingram Micro's Managed Firewall service. In Annex 1 you will find a summary of all the functions and content of the service.

2.1 SUPPORTED FUNCTIONS

The Managed Firewall service supports a wide range of functions. A distinction is made within the service between Managed Firewall Standard and Tailor-made.

The following functions are supported within the Managed Firewall service:

1. Edge firewall
2. Core firewall
3. SSL connections
4. IPsec connections
5. Web content filtering
6. Intrusion prevention
7. Anti virus
8. Anti spam

The use and possibilities of the above functions differ in the service models Standard and Tailor-made.

2.1.1 Edge firewall

An "Edge" firewall is placed at the edge of the network where the connection to all connections take place such as an internet connection. Think of firewalls at, for example, office locations where connections need to be safely accessed. Various security functions are activated here. The functionality offered by the firewall depends on the brand, type and associated licenses.

Within the service a distinction is made between two types of Edge firewalls.
Based on end-user and/or bandwidth usage.

The smallest variant Edge 1, is for an environment that serves fewer than 25 end users simultaneously and/or less than 20Mbit/s of bandwidth.

The Edge 2 firewall is for an environment where more than 20 Mbit/s bandwidth is consumed or more than 25 simultaneous users are served.

The Edge firewall function applies to the Basic and Standard service variants.

2.1.2 Core Firewall

When the firewall is placed in the "Core" of the network it becomes a critical element within the network. An example of a Core Firewall is a firewall environment that is centrally located in the data center. This positioning makes it possible to monitor and control all traffic within the network. The firewall is thus the conductor within the network and is able to scan traffic for unwanted behavior.

The Core firewall function applies to the Standard variant.

2.1.3 SSL connections

SSL connections are secure connections that are offered to employees or external parties to securely access IT services and/or infrastructure. By using an SSL client (software) a secure (SSL) connection can be established. As additional security, it is possible to use a personal token so that, in addition to the username and password, one also has to enter a unique code. The use and management of an additional token functionality is not part of the service.

The management of the SSL functionality is offered in the Basic and Standard service variants.

2.1.4 IPsec connections

IPsec connections may be required when locations need to be connected to communicate securely between location A and B. A firewall often has several of these connections. This traffic can be monitored by the firewall for unwanted behavior and content.

Ingram Micro is responsible for the configuration and monitoring of the IPsec connection(s) on the contracted firewalls. If a connection needs to be made to a firewall that is managed by a third party and/or client, the responsibility for configuring the IPsec connection lies with the third party and/or client.

The management of the IP-Sec connections is offered in the Basic and Standard service variants.

2.1.5 Web content filtering

Web content filtering is a functionality within the firewall that continuously scans the content of websites for unwanted behavior. By applying web content filtering, end users are protected as much as possible against harmful actions that can take place on websites. This blocks unsafe or undesirable content. The management of the policy and functionality is part of the service. The firewall should support this function. The licensing of the firewall is the responsibility of the client.

Web content filtering is supported in the Basic and Standard service variants.

2.1.6 Intrusion Prevention

Organizations often store their data in the public or private Cloud or data center. This data may only be accessed by authorized staff. To know if this has happened Intrusion Prevention is the mechanism that controls this. Hackers often use certain techniques that are recognized by this feature making it more difficult for a hacker to access this data.

The firewall should support this function. Licensing of the firewall is the responsibility of the client. Intrusion Prevention is supported in the Basic and Standard service variants.

2.1.7 Anti Virus

Anti virus functionality scans traffic for behavior and known malicious data. When data is recognized as a virus, this mechanism intervenes and blocks it. The firewall should support this function. Licensing of the firewall is the responsibility of the client. Anti virus is supported in the Basic and Standard service variants.

2.1.8 Anti spam

By applying this functionality, attempts at phishing and unwanted advertising are prevented as optimally as possible. The firewall should support this function. Licensing of the firewall is the responsibility of the client. Anti spam is supported in the Basic and Standard service variants.

2.2 HARDWARE

2.2.1 Supported brands

Ingram Micro supports all firewall devices that fall under the business segment in its services and can be managed remotely. Ingram Micro has the right to exclude equipment that cannot be managed properly in order to provide a quality service.

Ingram Micro can offer higher quality and a broader range of services if the Basic or Standard variants of Ingram Micro in the field of firewall equipment is chosen. Ingram Micro carries the network line of Fortinet, Cisco Enterprise and Cisco Meraki as standard. All Network Consultants and Engineers are trained and certified for this.

The service *Managed Firewall Basic applies if it concerns equipment of the brand "Cisco Meraki" and the service Managed Firewall Standard if it concerns equipment of the brand refers to "Fortinet" or "Cisco".*

2.2.2 RMA & Replacement

With *Managed Firewall Basic and Managed Firewall Standard* Ingram Micro takes care of the entire RMA handling of faulty hardware. When reporting (near) hardware defects, Ingram Micro will take care of the entire RMA process with Fortinet or Cisco / Meraki.

The on-site replacement of the hardware will be charged on the basis of post-calculation. The client can also choose to replace the hardware himself. Ingram Micro is at all times the coordinator of the RMA process.

If the device that needs to be replaced is at a certain height, an external organization will be called in. This is for the safety of our personnel. The costs of this will be charged on the basis of post-calculation.

A hardware support contract from the vendor is a basic condition on these services.

2.2.3 Architecture and advice

With *Managed Firewall Basic and Managed Firewall Standard,* it is possible to be relieved of any worries regarding architecture and advice concerning hardware replacement. This offers the advantage that you, as a customer, can outsource everything to one organization, and your own organization or a third-party organization does not have to be deployed for this. The condition is that the hardware must be from the brand Fortinet, Cisco, or Cisco Meraki.

Architecture and advice is optional with the Basic service variant and is included in the Standard service variant.

2.2.4 Cabling & peripherals

Ingram Micro can also relieve you from taking care of the installation and replacement of cabling and peripherals. This may include physical cabling, patch cabinets, cable ducts and finishing. This service is provided with the help of an Ingram Micro partner. Ingram Micro will be the coordinator at all times. The costs of this will be charged on the basis of post-calculation.

2.3 MONITORING & RESPONSE

The Ingram Micro Network Operating Center, hereafter referred to as NOC, is responsible for monitoring and managing the network environment.

The monitoring of the network is carried out by standard monitoring software of the relevant supplier / vendor via the "Basic" variant of the service, or by our high-end network monitoring environment based on from Auvik via the "Standard" service. For both variants, this is combined with the knowledge of specialized Network Administrators and Consultants.

The Auvik monitoring software that is used has been specifically developed for the management of network infrastructures. Ingram Micro not only has insight into the network infrastructure, but also what equipment is connected to the network. In this way Ingram Micro can also see what equipment is connected to the network, in addition to the network. This has the advantage that all equipment that is connected to the network and connected via an IP address can be tracked in the network.

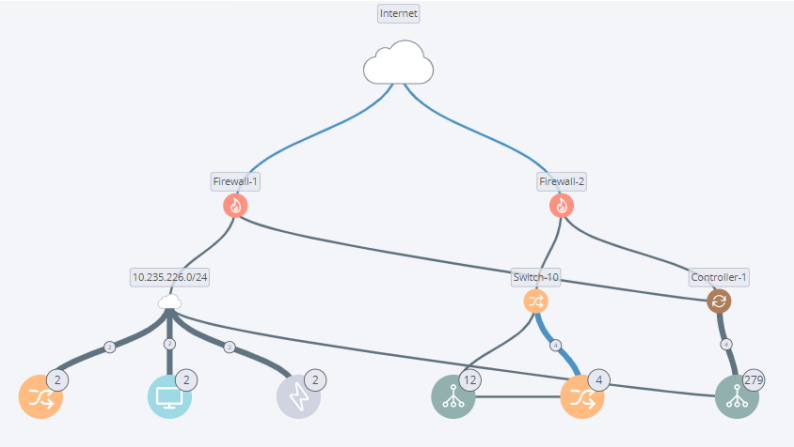

Figure 1: Example - Visualization physical network chain within Auvik

The building blocks on which Ingram Micro measures consists of the following components:

1. Availability
2. Utilization
3. Bandwith & Traffic

Alerting

Based on predefined parameters, the monitoring software issues an alert to which the NOC will directly respond within the SLA agreements. Depending on the type of failure and impact, the system creates an automatic classification. The NOC of Ingram Micro then determines the priority with which the incident will be dealt with, based on the client's specific situation (business impact). Determining the priority of the incident is always done in cooperation with the client. A single firewall that fails can have a major impact on the business operations. More information on prioritization in case of incidents can be found in the Service Level Agreement (SLA) of Ingram Micro.

Data retention period

The monitoring and configuration data of the systems is stored for a maximum of 10 years based on the current contract. If the contract expires or is terminated, the monitoring information in all the systems will be permanently deleted by Ingram Micro.

2.3.1 Availability

The most important component of monitoring is the availability of the network. Availability is determined by multiple factors within the network. The combination of these factors determines whether or not the service is available. Ingram Micro monitors the availability of each network device in order to measure the full availability.

The following availability units are measured continuously:

- Hardware device
- Port(s) and connections
- Administrative configuration
- Operational configuration
- Back-up
- Login
- SNMP

Availability is the most important parameter within the service. The availability of the equipment is reported every quarter.

2.3.2 Utilization

The utilization, also known as consumption of available resources, is measured continuously to ensure the availability, but especially to be able to interpret patterns and analyze problems properly.

The following utilization parameters are measured:

- Processor usage in %
- Memory usage in %
- Storage in % (if applicable)
- Port usage in %

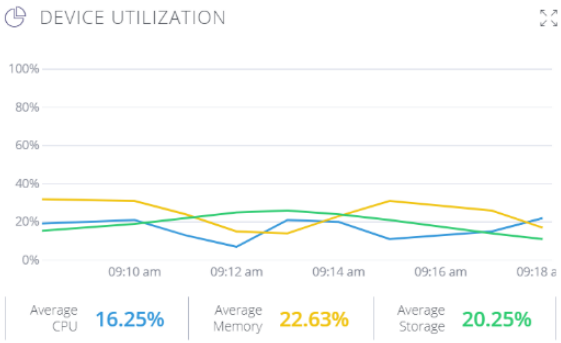

Figure 2: Example device utilization.

2.3.3 Bandwith & Traffic

All traffic handled by the managed firewall equipment is continuously measured by Ingram Micro's systems or the vendor.

The following parameters are only in the Standard variant proactively continuously measured:

- Bandwidth per device - Average Mbit/s
- Bandwidth per interface - Average Mbit/s
- Data packets per device - Number averaged per second
- Data packets per interface - Number averaged per second
- Loss of data packets per interface - Number averaged per second

Traffic is continuously measured for behavior and if inconsistent changes occur according to the system, alerts will be triggered based on the expected impact.

Certificate management, Multi-vendor Monitoring and the Intelligent Monitoring platform and learning is only included in the Standard variant.

2.4 PATCH & RELEASE MANAGEMENT

In order to guarantee the safety and functionality of the network, it is important to keep track of the firewall equipment in terms of firmware.

Ingram Micro makes a distinction in the following types of updates:

1. Security patches
2. Functional Updates

With *Managed Firewall Basic and Managed Firewall Standard the security patches, updates and functional upgrades are secured in the service.*

2.4.1 Security patches

The security patches are released by hardware suppliers to fix vulnerabilities and bugs. Ingram Micro monitors all firewall equipment and keeps track of *Managed Firewall Basic and Managed Firewall Standard whether necessary patches have been found for the firewall equipment.* Ingram Micro will roll out the security patches deemed necessary by the supplier to guarantee security and availability. If one or more security patches need to be installed, the change management process is launched to provide the network equipment with the necessary firmware.

2.4.2 Functional Updates

Network suppliers regularly release new functionalities on network equipment. Ingram Micro classifies these updates as functional updates. Functional updates are always carried out on the basis of a non-standard change and is part of the service with *Managed Firewall Basic and Managed Firewall Standard.* A functional update is only performed at the request of the client or on the recommendation of Ingram Micro.

2.4.3 Maintenance Window

With Managed Firewall Basic and Managed Firewall Standard, the proactive maintenance is carried out in consultation with the Client in view of the business-critical nature of the service provision.

2.5 BACKUP & RESTORE

All firewall equipment managed by Ingram Micro under the Managed Firewall service is included in our backup service. This functionality is provided in both Basic and Standard variants of the management service, with the exception of the export of device configuration(s) and the configuration history storage. The latter two are only available in the Standard variant.

2.5.1 Back-up

Every firewall device managed by Ingram Micro is automatically backed up. Any change made to the firewall device is automatically stored within the service.

In addition to the automatic backup of the equipment, all configurations are stored indefinitely. With this functionality, you can always look back at configurations and automatically compare them with each other. Also, if an external party submits a change request that is, for example, unsuccessful, it is very easy and quick to return to the last working configuration.

The backup function can be provided if the firewall is supported by Ingram Micro's management software and the firewall can be accessed remotely using the SSH protocol. The Telnet protocol is not supported.

If any of these conditions are not met, Ingram Micro cannot guarantee the backup of the firewall equipment.

2.5.2 Restore

Restoring the configuration (backup) of a network device is a standard in the service. This situation occurs, for example, in case of human failure or replacement of a firewall device.

The restoration of a configuration is always carried out under the direction of and by Ingram Micro in order to guarantee continuity. In case, for whatever reason, the configuration has been changed by a third party other than Ingram Micro, restoring a backup will always be charged based on post-calculation.

2.5.3 Export configuration(s)

Within the service provision of the variant *Managed Firewall Standard it is possible to request an export of the configuration of one or more network devices.* The costs of this will be charged on the basis of post-calculation.

3 Service Levels

The general service levels of Ingram Micro are described in the Service Level Agreement (SLA). This service description states which matters specifically apply to the Managed Firewall service.

3.1 SERVICE WINDOW

In the Managed Firewall service, there are two types of Service Windows available:

- Office hours
- 24x7 Prio 1 support

24x7 Prio 1 support is optional and is calculated over all firewall devices defined/contracted within the service.

3.2 CONFIGURATION MANAGEMENT

Ingram Micro is responsible for the administration of the following configuration items of all equipment managed by Ingram Micro:

Configuration Items*		
Device name	Serial number	Disc(s) (if applicable)
Device type	Firmware version	Work memory
IP addresses	VPN Tunnels	Network interfaces
Networks	User names	
Brand	Passwords	
Model	Cluster/Stack configuration	
Software version	CPU(s)	

** If the equipment does not have one or more configuration items or cannot be read, these configurations are not maintained by Ingram Micro.*

3.3 REPORTING

3.3.1 Portal

The Client gains insight into the following components by means of the portal:

1. Availability
2. Incident overview and KPIs
3. Change overview and KPIs

3.3.2 Trend analysis and advice

A trend analysis is created once every quarter within the *Managed Firewall Standard* service with relevant advice. The trend analysis and advice will be discussed personally with the client in order to jointly improve the service at Ingram Micro, the client and any third parties.

The trend analysis and proactive advice is only provided with *Managed Firewall Standard.*

4 Terms and Conditions

4.1 COPYRIGHT

4.2 DISCLAIMER

In compiling this service description, the greatest care has been taken to ensure the accuracy of the information contained herein. However, Ingram Micro cannot be held responsible for any incorrect information provided through this service description.

4.3 GENERAL TERMS AND CONDITIONS

The services are performed under the applicability of the NL Digital Terms and Conditions, as filed at the Central Netherlands Court, location Utrecht and which can be consulted on our website.

In addition to the General Terms and Conditions used by Ingram Micro B.V., the contractual Terms and Conditions laid down in the agreement that is concluded apply.

4.4 CONTACT DETAILS INGRAM MICRO

Ingram Micro B.V.
Papendorpseweg 95
3528 BJ Utrecht
T: +31 (0) 30 246 40 01

5 Annex 1: Service Matrix

MANAGED FIREWALL

√ Included

O Optional / Non-standard change

- Not possible / Not applicable

	BASIC		STANDARD	
SUPPORTED FUNCTIONS	Edge	Core	Edge	Core
Edge firewalling	√	*not applicable*	√	-
Core firewalling / routing	√	*not applicable*	-	√
SSL connection	√	*not applicable*	√	√
IP-sec connections	√	*not applicable*	√	-
Content Filtering(1)	√	*not applicable*	√	√
Intrusion Prevention(1)	√	*not applicable*	√	√
Anti Virus(1)	√	*not applicable*	√	√
Anti Spam(1)	√	*not applicable*	√	√
HARDWARE				
Supported brands (2)	Cisco Meraki	Cisco Meraki	Cisco ASA and Fortinet	Cisco ASA and Fortinet
RMA & Replacement (3) (4)	√	*not applicable*	√	√
Architecture & advice	O	*not applicable*	√	√
Cabling & peripherals	O	*not applicable*	O	O
MONITORING & RESPONSE				
Availability	√	*not applicable*	√	√
Utilization / Usage	√	*not applicable*	√	√
Bandwidth & Traffic	-	*not applicable*	√	√
Certificate management	-	*not applicable*	√	√
Multi-vendor monitoring	-	*not applicable*	√	√
Intelligent Monitoring platform and learning	-	*not applicable*	√	√
BACKUP & RESTORE				
Automatic Backup	√	*not applicable*	√	√
Restoring Backup	√	*not applicable*	√	√
Configuration history storage	-	*not applicable*	√	√
Export device configuration	-	*not applicable*	√	√
SECURITY & COMPLIANCE				
ISO 27001 - Information security	√	*not applicable*	√	√
ISO 9001 - Quality Management	√	*not applicable*	√	√
NEN 7510 - Information security Healthcare	√	*not applicable*	√	√
ISAE 3402 TYPE 2 - Outsourcing standard	√	*not applicable*	√	√
PATCH & RELEASE MANAGEMENT				
Security updates (4)	√	*not applicable*	√	√
Functional Updates (4)	√	*not applicable*	√	√
SUPPORT				
Office hours; 08:00 - 18:00	√	*not applicable*	√	√
24/7 - Prio 1 Support	O	*not applicable*	O	O

REPORTING				
Incident overview & KPI's - per month (via portal)	√	*not applicable*	√	√
Change overview & KPI's - per month (via portal)	√	*not applicable*	√	√
Trend analysis & Advice - per quarter	-	*not applicable*	√	√

1 Hard- and software should support the function

2 Equipment must be remotely reachable/accessible

3 Replacement at additional cost.

4 Hardware support contract is required

6 Annex 2: System requirements & preconditions

6.1 MANAGEMENT SERVER MONITORING SOFTWARE

Description	Requirement
Operating system	Windows 7+ or Windows 2012+
(v)CPU	At least 1 vCPU
Work memory	At least 2GB
Storage	At least 8GB
Internet connectivity	At least 5mbit/s
FIREWALL connectivity	Connection internal network

6.2 FIREWALL RULES MANAGEMENT SERVER TO INTERNET

URL's	Ports / configuration
*.amazonaws.com	80 & 443
*.security.ubuntu.com	80
*.google.com	80 & 443
DNS	8.8.8.8:53 & 8.8.4.4:53
NTP - Policy required	pool.ntp.org:123

6.3 FIREWALL RULES MANAGEMENT SERVER - INTERNAL NETWORK

Protocols	Ports
HTTP	80 & 8080
HTTPS	443 & 8443
DNS	53
NTP	123
BGP (Border Gateway Protocol)	179
FTP (File Transfer Protocol)	21, 115, 10021
Java	9010
OSPF (Open Shortest Path First)	89
RADIUS (Remote Authentication Dial-In User Service)	1812
SMTP (Simple Mail Transfer Protocol)	25
SNMP (Simple Network Management Protocol)	161
SSH (Secure Shell)	22
Syslog	514, 54059
TCP Health Check	12345
TFTP (Trivial File Transfer Protocol)	69, 10069
Telnet	23
UPnP (Universal Plug and Play)	1900
mDNS (Multicast DNS)	5353