Every day, companies are confronted by a wide range of threats and dangers from the Internet. To achieve optimal protection, they need to step up from a conventional firewall to multi-functional protection.

The MSS-i Managed Firewall offers comprehensive, integrative and proactive protection within a single system. This powerful security solution provides protection from known and unknown threats.
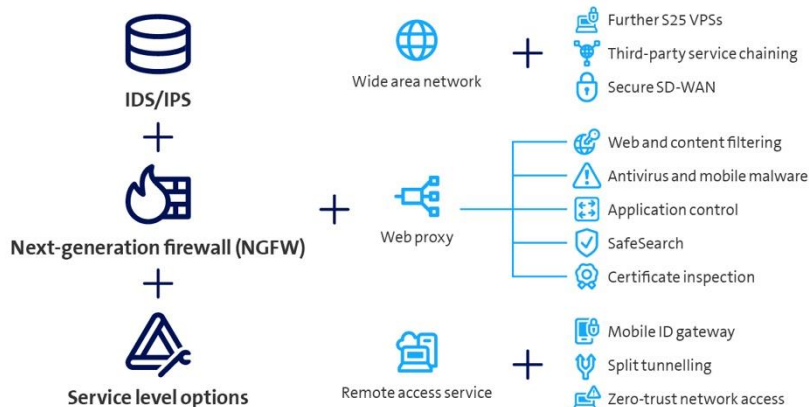The MSS-i Managed Firewall offers flawless convergence that can be individually scaled for any location, such as remote office, branch, headquarters, data centre, Swisscom cloud and public cloud. The MSS-i Managed Firewall service is integrated together with the customer and run by the Swisscom Security Operation Centre. The basic next-generation firewall service can be supplemented with the extended services wide area network (WAN), web proxy or remote access services, and combined with other options such as UTM protective functions, secure SD-WAN or zero-trust network access. The MSS-i customer portal is the central, digital access for the managed firewall service. Simple adjustments to the managed firewall configuration can be implemented immediately and at any time via the optional self-service portal. The managed firewall service can be combined with further Swisscom security or connectivity services.

Your advantages with MSS-i Managed Firewall

Swisscom has an extensive team of experts for firewalls.

Swisscom sets up and runs firewalls from a globally leading provider of security solutions.

Based on the system requirements, the corresponding physical or virtual firewalls are deployed with the necessary accessories.

Swisscom takes care of the professional coordination and integration of the managed firewalls, drawing on the security requirements of the customer.

The Swisscom Security Operation Centre handles all operational tasks up to 24/7, supporting customers in case of questions or adjustments with qualified experts.

The MSS-i customer portal offers the customer easy access to the managed firewall service and simplifies communication and adjustments with the Swisscom Security Operation Centre.

Services at a glance

IDS/IPS
+
Next-generation firewall (NGFW)
+
Service level options

Wide area network
+
Further S25 VPSs
Third-party service chaining
Secure SD-WAN

Web proxy
Web and content filtering
Antivirus and mobile malware
Application control
SafeSearch
Certificate inspection

Remote access service
+
Mobile ID gateway
Split tunnelling
Zero-trust network access

Facts & Figures

Basic service Next-generation firewall (NGFW)

Standard service
Stateful Layer 4 firewall with NAT/PAT, routed mode and standard rule set.

Provision
Local, Swisscom clouds or in public clouds (Azure, AWS)

Project and operation services including customer portal over the agreed contract term
Support hours: 5×11h, 7:00 – 18:00
Availability: Best effort (single node)

Additional option*
IDS/IPS

The basic service is offered as a standard service (with or without options) with a fixed price for project and operation. Additional configurations* such as additional rule sets during the project phase are charged according to time and expense.

Service level options*

– Support hours: 7×24h, 0:00 – 24:00
– Availability: 99% or 99.9% (cluster node)
– Included tickets / hours pool for service requests
– Self-service portal
– Security monitoring with dashboard

Extended service Wide area network*

Standard service
Hub and spoke S2S VPN with static routing and standard rule set.

Additional options*
– Further S2S VPNs
– Third-party service chaining (e.g. partner VPN, Zscaler)
– Secure SD-WAN

The wide area network* (WAN) extended service is offered as a standard service (with or without options) with a fixed price for project and operation. Additional configurations* such as dynamic routing are additionally charged according to time and expense in the project phase.

Extended service Web proxy*

Standard service
Explicit or transparent forward proxy with web and content filtering, antivirus, mobile malware, application control, SafeSearch including certificate inspection.

The web proxy extended service is offered as a standard service with a fixed price for project and operation. Additional configurations* such as SSL inspection are additionally charged according to time and expense in the project phase.

Extended service Remote access services*

Standard service
Design, implementation and acceptance of gateway with authentication interface including RAS clients per device.

Additional options*
– Mobile ID gateway (additional mobile ID contract required)
– Split tunnelling
– Zero-trust network access

The remote access service extended service is offered as a standard service with a fixed price for project and operation. Additional configurations* during the project phase are charged according to time and expense.

* Paid additional services