Managed Firewall Service

So that not just anybody can access and leave your sites at will

Protect your company network reliably against attacks from the Internet. With the Managed Firewall Service, you benefit from basic port handling and many other functions.

The following services are an integral service component:

Network address translation (NAT)

Changes the IP address information of packets at the firewall. This means that, during a session, the firewall is the only instance that contains all the address information.

Stateful inspection

Covers spoofing and packet filtering. Spoofing refers to methods that are used to suppress authentication and identity procedures if these are based on the use of trusted addresses or host names in network protocols. Packet filtering is a dynamic filtering technique that assigns every data packet to a session. The packets are analysed and saved in dynamic condition tables. Packets that cannot be assigned to pre-defined contacts or may belong to a DoS attack are discarded.

Zone-based policy

The source and destination addresses are checked. The provision of a source and a destination zone is additionally requested. If a source is not in the assigned zone, the firewall discards the packet.

Performance tuning

Maximises the performance of systems. Here, an optimal and up-to-date policy is required, as well as specific settings on the firewall.

Virtual local area network (VLAN)

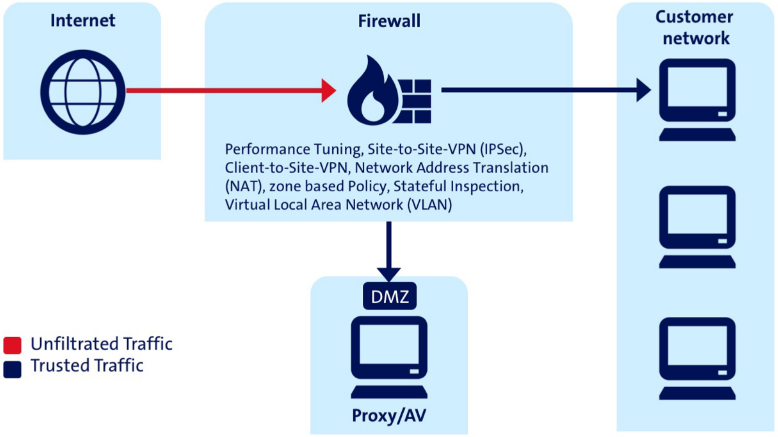
Logical partial network within a physical network. Data packets from the firewall, router and switches are forwarded to partial networks.

Clustering

With the appropriate service level agreement, a cluster consisting of two managed devices is installed. The cluster can be set up at one site or distributed across several sites. It is operated based on an active/passive model.

VPN (site-to-site)

We use the IPSec protocol to ensure a secure connection between two sites. The prerequisite for this is that the sites are connected by a network (Internet, MPLS, etc.). In most cases, the Internet is used as the means of transfer. This connection can be established with a partner firewall or with Swisscom's Managed VPN service.


Internet
Firewall
Customer network
Performance Tuning, Site-to-Site-VPN (IPSec), Client-to-Site-VPN, Network Address Translation (NAT), zone based Policy, Stateful Inspection, Virtual Local Area Network (VLAN)
DMZ
Proxy/AV
🟥 Unfiltrated Traffic
■ Trusted Traffic

Optional additional services

VPN (client-to-site)

To ensure secure company access for your end users, we offer a client-to-site solution based on the SSL protocol. Security settings are defined on the gateway for each profile. Straightforward user authentication (user/password) can be ensured by means of connecting to your directory server (ADS, Radius, etc.).

VPN (client-to-portal)

Using a Web portal you can provide your partner with secure access for a large number of your company applications. You do not need to provide the partner with any terminals.

Strong authentication

Increased access security through two-factor authentication with user name and password as well Mobile ID or a one-time token (SMS, SW and HW token) as a second factor. User administration and reporting are carried out using an eService portal.

Quality of service

The data package arrives at the firewall with a DSCP value. The firewall prioritises this data package in accordance with the DSCP value. The DSCP value is not changed. The prerequisite for this option is that the customer has an end-to-end QoS concept into which the firewall is integrated.

Recurring services

Health Incident Monitoring and Management	Swisscom guarantees that health incidents are processed within the defined service level times. If a security device cannot be reached, Swisscom resolves the problem and informs you immediately.
Security Incident Monitoring and Management	The log data from the firewall is used to create events, which are analysed for threats using the Threat Intelligence function. In the event of a suspicion, a security incident is created and assigned to one of several classes (Insufficient Info, Harmful Attack, Harmless Attack, False Positive). The Insufficient Info and Harmful Attack classes are analysed by a specialist and specifically escalated to you.
Change Management	You assess the urgency of implementing a change. Swisscom distinguishes between minor and major changes. Minor changes are part of the service. These are requested directly in the MSS-i dashboard.
Release Management	Swisscom tests the manufacturer releases of managed devices in the laboratory in accordance with a defined test catalogue and, following approval, implements them. In the case of the VPN client, only basic connectivity tests are performed at the gateway.
Vulnerability Management	When a critical weakness of a managed device is published, Swisscom takes a proactive role, informing you and ensuring that the weakness is eliminated in accordance with best practice.
Configuration and Backup Management	Swisscom takes care of all current configurations and ensures that backups are stored securely and clearly. This allows older configurations to be restored when required.
Life Cycle Management	Swisscom uses only hardware and software that is state of the art.
Reporting	You can compile detailed reports individually via the MSS-i dashboard. In accordance with the service level, the availability, ticket status (Incident and Change Management) and management reports are created automatically.

Service options	
Support hours 7x24	●
Support hours 5x11	○
Security dashboard	●
Service level	Standard, Premium Platinum
Data retention - log data and requests: 1 year	●
Data retention - backup: 30 days	●

● = Standard ○ = optional ⊙ = subject to extra charge

Technical features	
Release management incl. testing	●
Vulnerability management	●
Automated log analysis for security incidents	●
Individual policy	○
On-premise device	●
Virtual device	○
Read-only access	⊙
Sending log data to Syslog server	⊙
Client-to-site VPN	⊙
Client-to-portal VPN	⊙
Authentication (LDAP, RADIUS, certificates, strong authentication)	⊙
Intrusion detection system (IDS)	⊙

● = Standard ○ = optional ⊙ = subject to extra charge

Swisscom, the ideal partner

Swisscom runs a Swiss operations center for network security. This features round-the-clock support from qualified experts, permanently up-to-date certifications and threat intelligence that is optimized for Switzerland. It is the ideal security solution for Swiss companies.

Further information on the service can be found in the info box and at www.swisscom.com/mss-i

How you benefit

- You know that your firewall is always up to date.
- The firewall log data is analysed by means of Threat Intelligence.
- You can integrate the service into your structure and supplement it with modules at any time.
- Protection for virtual servers within the Dynamic Computing Service can be provided by MSS-i.
- The MSS-i dashboard constantly keeps you informed of the status of your service.
- You benefit from real-time monitoring round the clock by qualified security experts.