Managed UTM Service (Unified Threat Management)

Managed UTM provides your company with optimum protection against dangers from the Internet. This allows you to increase the protection level from a traditional firewall to multifunctional protection.

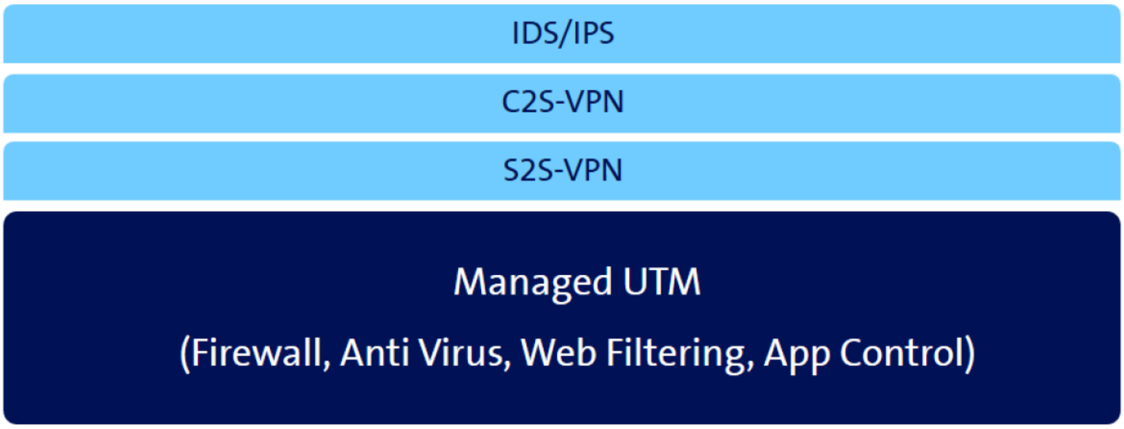
Stateful inspection
Covers spoofing and packet filtering. Spoofing refers to methods that are used to suppress authentication and identity procedures if these are based on the use of trusted addresses or host names in network protocols. Packet filtering is a dynamic filtering technique that assigns every 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 provision of a source and a destination zone is requested in addition to a source and destination address. If a source is not in the assigned zone, the firewall discards the packet.

Anti virus
A policy is used to decide which protocols are examined for viruses, malware or other damaging software. Swisscom uses a standard policy that works in accordance with best practice. The signature database is updated automatically on a regular basis and is monitored.

Web filtering
The manufacturer divides all known websites on the Internet into categories. Using a standard policy, Swisscom blocks access to specific categories. It is possible to release individual blocked URLs in the categories. Swisscom uses the categories and subcategories of the service that are provided by the manufacturer.

Application control
The application control function is used to permit or block access to the application. Swisscom blocks pre-defined application categories. At the customer’s request, further categories can be blocked or individual applications permitted.



IDS/IPS

C2S-VPN

S2S-VPN

Managed UTM

(Firewall, Anti Virus, Web Filtering, App Control)

Optional additional services

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.

VPN (client-to-site)

To ensure secure access to the company network 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.).

IDS/IPS

To protect the company network, communication is safeguarded using a best practice signature set from Swisscom. This contains signatures for the protection of incoming and outgoing data traffic.

Hybrid UTM (cloud-based)

Performance-intensive features such as URL filtering, anti-virus protection and sandboxing are provided in the Swisscom cloud. The Swisscom cloud is located in Swiss data centers and is operated from Switzerland. This reduces the burden on premise-based systems, and the systems can be scaled even with rapidly increasing user numbers and worldwide distribution.

Recurring services

Health Incident Monitoring und 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 suspected threat, the system creates a security incident which is divided up into different classes (insufficient info, harmful attack, harmless attack, false positive). The classes "insufficient info" and "harmful attack" are analysed by an expert and escalated to you in a targeted way.
Change Management	You assess the urgency of implementing a change. Swisscom makes a distinction between minor and major changes. Minor changes are an integral service component. 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.
Signature and category of management proxy, web antivirus and web filter management	The service includes the automatic updating of manufacturer updates such as signatures, categories and new applications. Signatures are imported into the system each day at off-peak times. Changes to the categories or applications are made at regular intervals. All changes are carried out according to best practice without a change request.
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.

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 (SLA: Premium, Platinum)	●
On-premise device	●
Virtual device	○
Read-only access	⊙
Sending log data to Syslog server	⊙
Site-to-site VPN	⊙
Client-to-site VPN	⊙
Intrusion detection system (IDS/IPS)	⊙

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

Swisscom, the ideal partner

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

Further information on the service: www.swisscom.com/mss-i

How you benefit

- You know that your systems are always up to date.
- You can integrate the service into your structure and supplement it with modules at any time.
- 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.