Managed IDS/IPS service

To make sure you're the first one to know when you have unwelcome visitors.

Swisscom uses «managed IDS/IPS» to detect and block data traffic dangerous for your company in real time on the basis of attack patterns and protocol anomalies.

Companies are regularly subjected to attacks.
An intrusion detection system (IDS) analyses and an intrusion prevention system (IPS) additionally blocks data traffic, thus reliably securing the infrastructures and applications. IDS/IPS checks the unencrypted data traffic in real time and sounds the alarm in the event of attack patterns and protocol deviations. Standards such as ISO 27001, PCI DSS and the recommendation of the FINMA require the systematic monitoring of unauthorised accesses. The following services are integral service components:

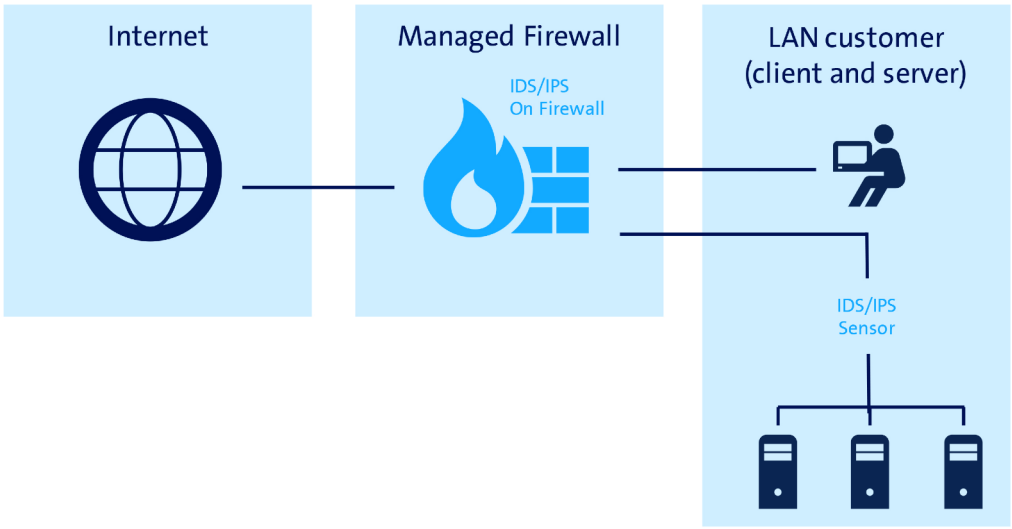
Best practice signature set
The managed IDS/IPS service is activated on a managed firewall or optionally as a standalone sensor. To protect the company network, communication is safeguarded using a best practice signature set from Swisscom. This contains signatures for the protection of incoming and outgoing data traffic.

IDS/IPS event analysis
In the event of abnormal data communication, the managed IDS/IPS service issues a warning and records the data communication, then classifies it and blocks it according to the policy. If the IDS/IPS system classifies a data communication process as an incident, the process is additionally analysed using Swisscom threat intelligence. Incidents are automatically displayed in the Security Dashboard and recorded. This ensures that any change made is given a time stamp.

The security experts at Swisscom analyse each incident classified as dangerous. If an incident is confirmed, the customer is informed of it and of possible countermeasures. Harmless incidents and incidents incorrectly classified as dangerous are saved.

Network or segment monitoring
The question as to whether IDS/IPS is to be activated for the entire network or for individual segments only is defined during implementation.

Reporting
Security events based on IDS/IPS signatures are visible in the Security Dashboard. In the case of critical attacks, they are escalated to the customer by means of a security incident. Further reports can be compiled in the Reporting Center.



Optional additional services

Standalone sensor
The managed IDS/IPS service is implemented on the basis of a separate sensor and can be activated at various points in the network.

Customer-specific signature set
In conjunction with the customer, an individual IDS/IPS profile is implemented in the customer environment.. To ensure that this profile remains up-to-date, regular proactive cooperation on the part of the customer is essential.

IPS
In conjunction with Swisscom, individual signatures or several signatures at once can be changed over from detect mode to prevent mode.

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 rectifies the fault and informs you immediately.
Security incident monitoring and management	From the log data of the IDS, events are created and then analysed for threats using threat intelligence. In the event of a 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.
Release management	Swisscom regularly tests manufacturer releases of the managed devices in the laboratory according to a defined test catalogue and implements them automatically after release.
Vulnerability management	When a critical weak point of a managed device is made public, Swisscom adopts a proactive role, informing the customer and ensuring that the weak point is eliminated according to best practice.
Signature management	Swisscom uses manufacturer signatures of the categories "critical" and "high" only. Manufacturer signatures are updated automatically at regular intervals The Swisscom best practice signature set is checked for changes every month and adapted accordingly. All of these changes are carried out according to best practice without a change request.
Life cycle management	Swisscom uses state-of-the-art hardware and software only.
Reporting	Detailed reports can be compiled individually via the MSS-i dashboard.

Service options	
Support time 7x24	●
Support time 5x11	○
Security Dashboard	●
Service Level	Premium Platinum
Data Retention – events: 1 year	●
Data Retention – backup: 30 days	●

● = Standard ○ = Option available

Technische Features	
Release Management incl. testing	●
Vulnerability Management	●
Automated log analysis for security incidents	●
Activated on firewall	●
Customer-specific signature set	⊙
Standalone sensor	⊙
IPS	⊙

● = Standard ⊙ = for an extra charge

Swisscom - the right partner

Swisscom maintains the Swiss operations center for network security. This provides round-the-clock support from qualified experts, certifications which are up-to-date at all times and threat intelligence optimised for Switzerland. It is the secure solution for Swiss companies.
For more information on the service, go to www.swisscom.com/mss-i

Here's how you benefit

- You ensure that unauthorised accesses are detected in real time.
- You detect known attacks thanks to signatures
- You filter relevant security incidents.
- You monitor the traffic behaviour of your organisation.
- You analyse encrypted and unencrypted data traffic.