



Managed Application Delivery

Making sure your web applications don't become a self-service store.

With the Managed Application Delivery Service, you ensure that your web applications are available to specified users. Internet users have access to the Application Delivery Controller (ADC), which simplifies access administration. The ADC takes care of routing to the relevant applications.

Traffic Load-Balancing

To dynamically distribute the request volume across different servers, load balancing is used. This permits queries to one IP address to be distributed across any desired number of IP addresses, allowing the response times of the servers to be improved considerably. This module can be used in an internal network or in combination with a ADC.

Reverse proxy

When a website is accessed, a connection is established from the client to the ADC. Incoming connections on the ADC are subjected to a basic check. Then the ADC establishes a new connection to the web server.

SSL Inspection

The web server is addressed using an encrypted protocol (HTTPS).

The encrypted connection is broken down on the load balancer and examined. Then a new encrypted connection is established to the destination server.

Reporting

Security events based on log data are visible in the Security Dashboard. In the event of critical attacks, they are escalated to the customer via security incidents. Further reports on events and incidents can be compiled in the Reporting Center.

Geo location enforcement

Access to your web server can be restricted to certain countries.

Application attack signatures

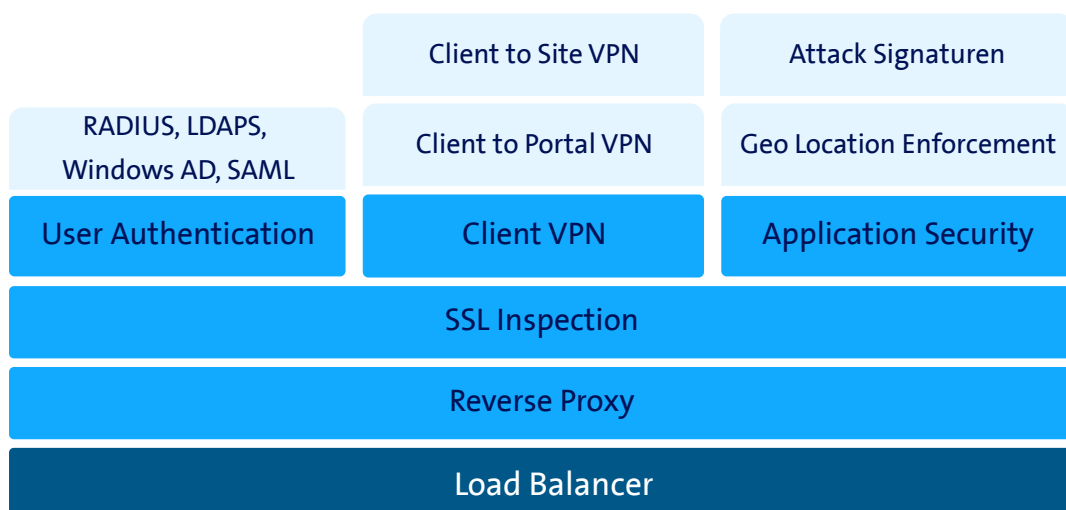
To provide protection from known attack patterns and weak points, the relevant signatures of the manufacturers used are activated. This blocks known attacks such as SQL injection.

User authentication

Single sign-on via various authentication protocols.

Client VPN

Client-to-portal VPN or client-to-site VPN to guarantee protected access for clients.



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	The log data from the ADC are 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 to different classes (insufficient info, harmful attack, harmless attack, false positive). The "insufficient info" and "harmful attack" classes 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.
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 directly requested in the MSS-i dashboard.
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.
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 times 7x24	●
Security Dashboard	●
Data retention - events and log: 1 year	●
Data retention - backup: 30 days	●

Technical features and options	
Release management incl. testing	●
Vulnerability Management	●
Automated log analysis for security incidents	●
Load balancing	●
Reverse proxy	⊙
SSL inspection	⊙
Geo location enforcement	⊙
Application attack signatures	⊙
User authentication	⊙
Client VPN	⊙

● = 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 safe solution for Swiss companies.

For more information on the service, see the information box or go to www.swisscom.com/mss-i