AIRLOCK

White Paper

Secure Reverse Proxy Server and Web Application Firewall

Contents

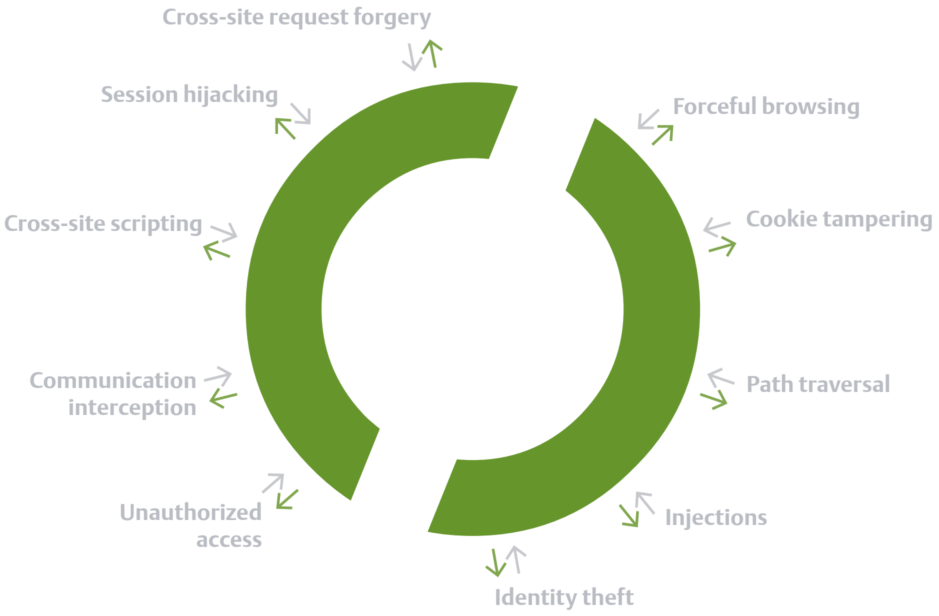
Losing control

The Internet allows sensitive data and transactions to be accessed directly using electronic means. Web applications are vulnerable at many different levels, even when priority has been given to addressing security at the development stage. The complexity of the attack scenarios and the increasing number of vulnerabilities in Web applications is leading to loss of control and extremely high levels of risk. Internet attackers have both commercial and criminal motivation. Systems that fall victim to a successful attack can deliver valuable data and make it possible to manipulate transactions, as well as providing the ideal platform for distributing malicious software (malware, viruses, Trojans) to unsuspecting users.

The consequences of an attack may include identity theft, access to confidential data, falsified transactions, poor availability and serious damage to an organisation›s reputation. The challenge facing companies today is how to get a handle on the security measures necessary to meet with compliance requirements and to guarantee the security of applications and data, with an acceptable expenditure of time, effort and money.

Online accessibility means vulnerability

When Web applications are developed, the primary focus is on business processes, not protection against attacks. In the best-case scenario, developers can take some action to mitigate against known modes of attack. As soon as the application is up and running in a live environment and new, previously unknown types of attack are deployed, it becomes necessary to apply security patches and updates to every application. An equally big challenge is faced by staff tasked with maintaining security: Web applications constantly reveal different weaknesses and are continuously bombarded with new attacks.

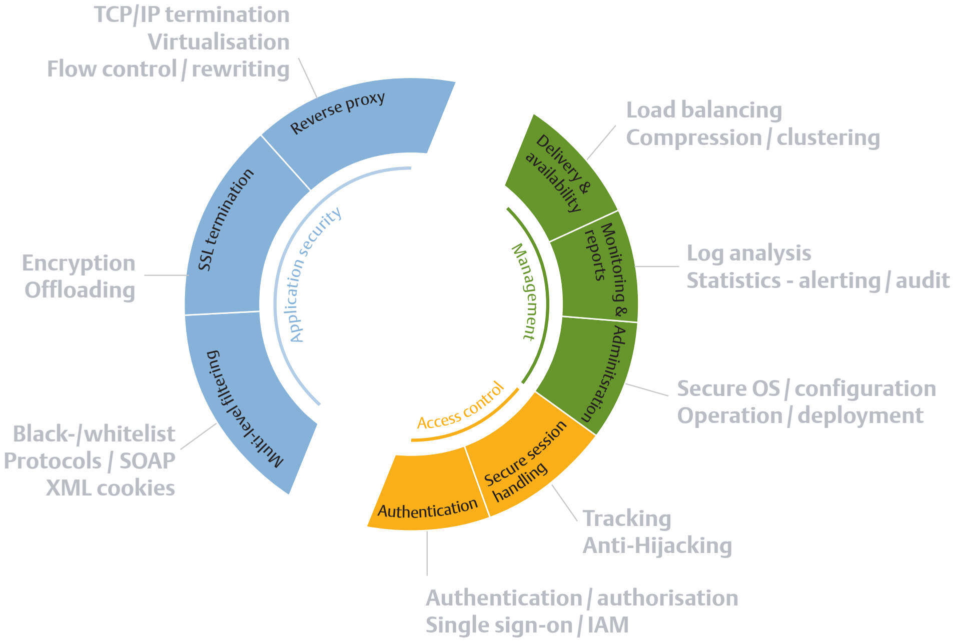


Regain control with a central access point

Because it acts as a central access point, Airlock gives staff responsible for security an important tool for maintaining control over their systems. Web applications and Web services are protected proactively. All requests and data are monitored at all times. Where necessary, specific URLs can be blocked. Operating as both a secure reverse proxy server and Web application firewall, Airlock offers a unique combination of protection mechanisms. All access attempts are systematically controlled and filtered at every layer. Moreover, Airlock can also force user authentication while allowing single sign-on and offering SSL VPN access. All important information is available through a range of monitoring and reporting functions. As the only Web application security solution on the market, Airlock covers every aspect of protecting and optimizing the complete Web environment.

Strategic security solution

A successful attack requires just a single vulnerability, which could be in any layer. Therefore, to be effective a Web applications security solution must provide simultaneous coverage in every relevant layer.

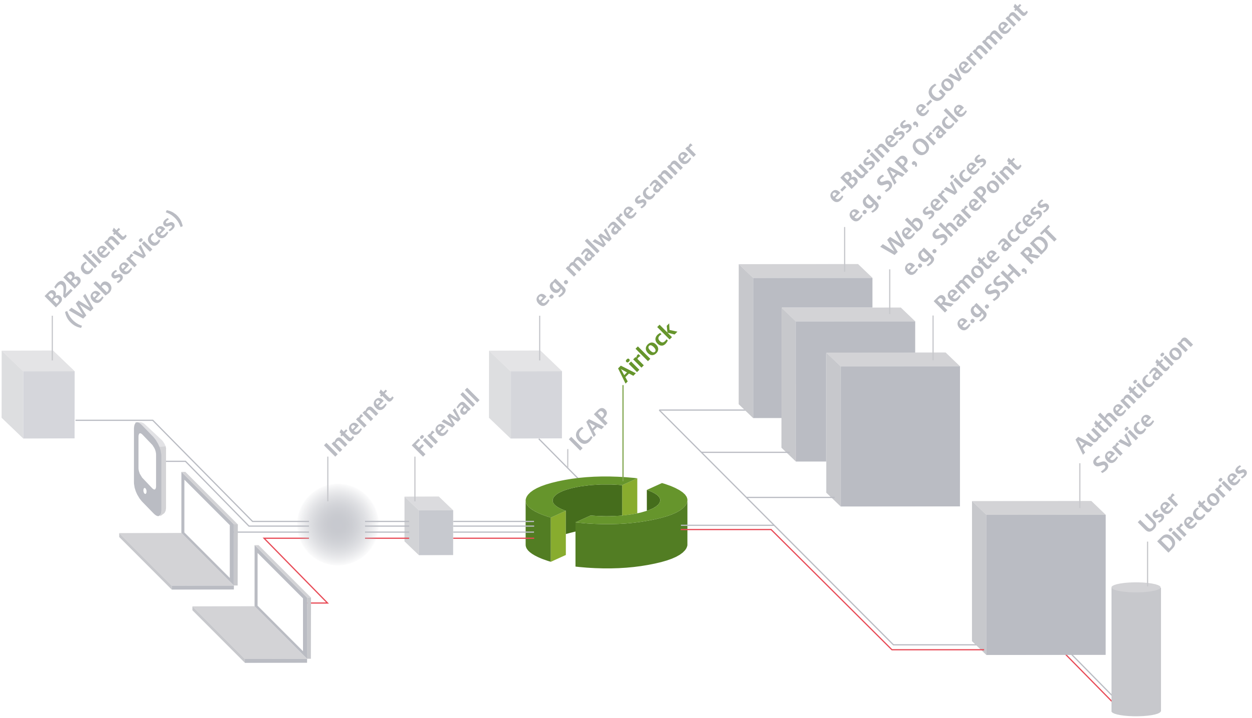


Secure communication

Operating as a reverse proxy server, Airlock actively ensures that all data connections that need protecting are encrypted and integrity-protected. By taking over this function, Airlock removes a heavy load from the Web and application servers. This results in increased application availability and performance and ensures that communications channels remain consistently secure.

Authentication and user sessions

When it comes to applications that require authentication of users, from a security perspective the issues of authentication and secure session control are much more important than any filter. Airlock therefore provides the ability to authenticate users upstream and conduct user sessions in a secure manner. This prevents anonymous connections to the application servers per se, thereby drastically reducing the scope of potential attacks. From a security point of view, decoupling authentication from the application logic is an important consideration. Airlock achieves this neatly, while still allowing the flexibility to choose an authentication method.

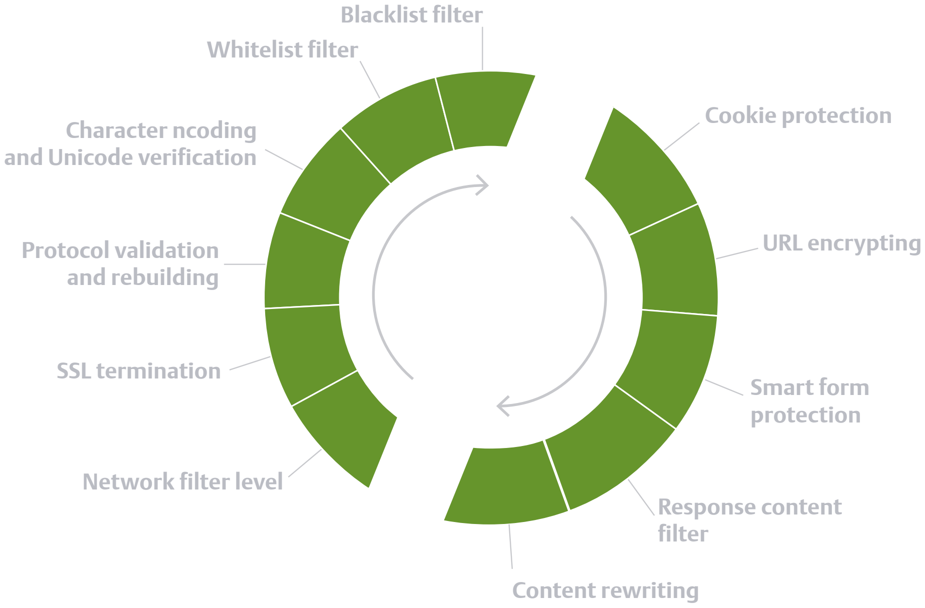


Access Control

Users should not necessarily be permitted to do everything, even after they have been authenticated. In combination with the preceding authentication, Airlock ensures at all times that users are only able to use those applications and functions for which they have authorisation. Working in conjunction with various different applications, single sign-on scenarios can be implemented that are highly attractive to users but do not compromise on the necessary security.

Filtering and acceleration

Web applications and Web services are nothing more than electronic interfaces to data and transactions. Because the browser displays the actual user application, attackers are able to communicate far too freely with the application server, allowing them to exploit vulnerabilities. Airlock functions as a central access point and performs strict filtering on all requests and data. Only requests that the system determines to be valid are passed to the application server. To determine the validity of requests, Airlock employs a range of techniques, including highly dynamic security functions:



Dynamic filter mechanisms, such as URL encryption, HTML form signatures and dynamic whitelists, offer the advantage that the Airlock filter configuration is automatically adapted to the application. Even if URLs change or parameters are renamed, the security checks will remain valid without the need to reconfigure any filters. Statically generated filter rules cannot respond to the dynamic behaviour of modern Web applications, even when they are generated using a so-called «learning mode».

Special techniques for network connection handling and support for real-time compression over HTTP/S deliver an additional level of acceleration that is noticeable to the user. The bandwidth requirement for the use of Web applications is also similarly reduced.

Virtualization of the Web presence

The internal architecture of a DMZ and the Web environment is often visible from the outside due to a lack of suitable precautions. This offers a potential attacker avoidable opportunities to easily obtain information. Thanks to the comprehensive reverse proxy functionality provided by Airlock, which also supports full rewriting of HTML and any other content, the Web environment that is presented to the outside world is fully virtualized. This makes the system extremely user-friendly, while at the same time reducing the size of the target exposed to attack.

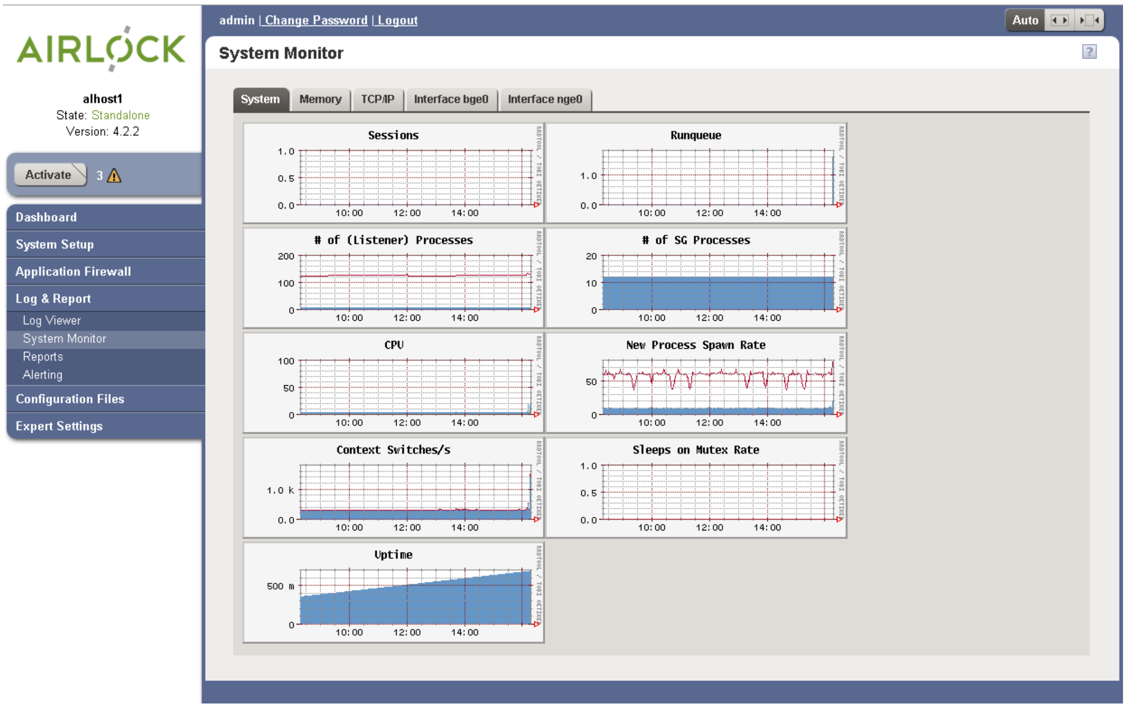
Load-balancing and failover

Additional security features for Web applications only really make sense when the availability of services can also be increased. Instead of having solutions for handling requests and sessions distributed across different application serves, Airlock offers this functionality directly. Indeed, functionality to ensure high availability of Airlock itself is also integrated into the system (failover cluster).

> «By using dynamic filter mechanisms, the Airlock filter configuration automatically adapts itself to the application. Even if URLs change or parameters are renamed, the security checks will remain valid without any need to reconfigure filters.»

Monitoring and reporting

Eliminating the need to fly blind is one of the greatest challenges that must be overcome when implementing security solutions. Because Airlock addresses every relevant layer of the system, it offers an unrivalled quality of data for use in reports and interactive monitoring. Whenever Airlock detects a security breach, all relevant data is immediately made available in the graphical reporting and monitoring tool. This information includes, for example, which user caused the breach during which session and what other actions that user carried out before and after the breach.



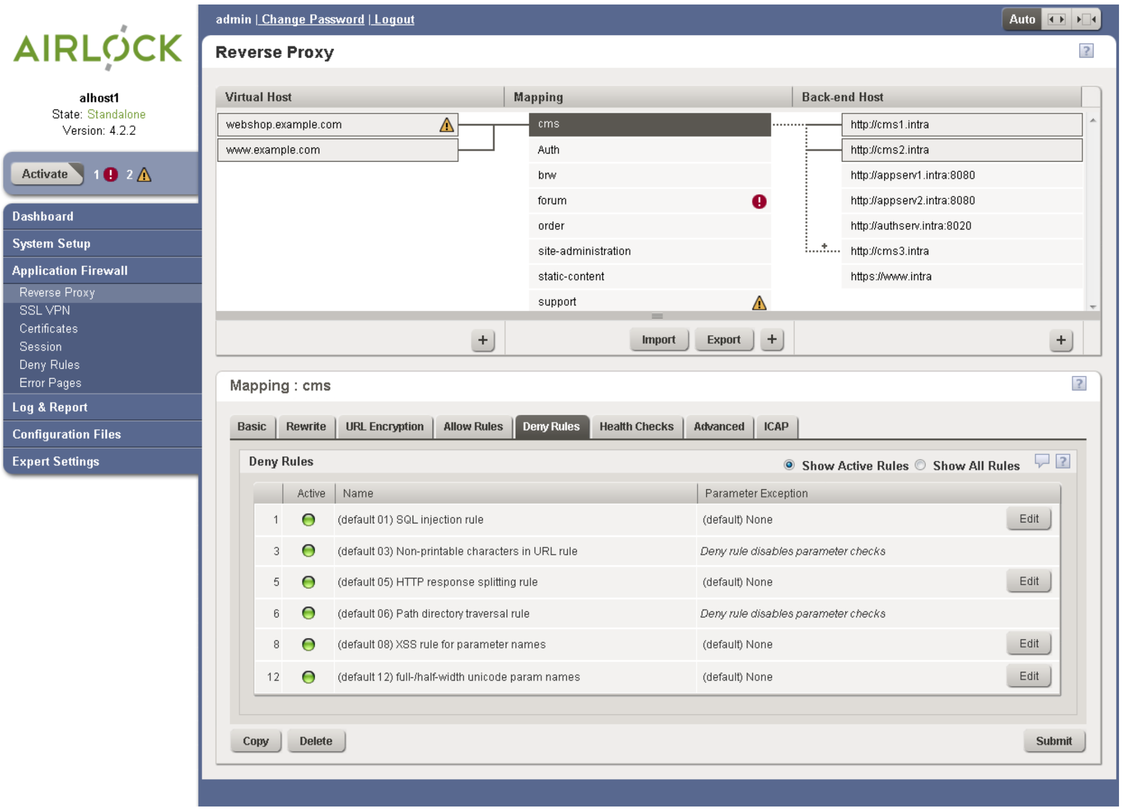
alhost1
State: Standalone
Version: 4.2.2

Flexible integration with associated systems

A central security solution does not operate as an isolated system, but rather interacts with numerous associated systems such as monitoring systems and user directories. In order to ensure that it integrates seamlessly with these other systems, Airlock operates at the protocol level and offers standardised interfaces The Airlock authentication service incorporates the most up-to-date authentication techniques and, whenever necessary, can easily be linked to any other authentication services that may be required.

Convenient, reliable configuration

Security solutions are often difficult to administer. The Web administration interface for Airlock was developed from the ground up to ensure that the system configuration process was convenient and reliable. Virtual hosts are linked graphically with mappings and back-end hosts. This means that it is always easy to get a good overview of the Web environment as it is presented to the outside user. A variety of administrator roles means that access powers can be separated. The system maintains a configuration version history, allowing rollback to a previous state to be carried out whenever needed. Various assistance features, such as the real-time regular expression tester and integrated comment fields, help simplify the configuration process and reduce overheads.



alhost1
State: Standalone
Version: 4.2.2

Reverse Proxy

Virtual Host	Mapping	Back-end Host
webshop.example.com ⚠	cms	http://cms1.intra
www.example.com	Auth	http://cms2.intra
	brw	http://appserv1.intra:8080
	forum !	http://appserv2.intra:8080
	order	http://authserv.intra:8020
	site-administration	http://cms3.intra
	static-content	https://www.intra
	support ⚠	

Mapping : cms

Deny Rules ● Show Active Rules ○ Show All Rules

	Active	Name	Parameter Exception	
1	●	(default 01) SQL injection rule	(default) None	Edit
3	●	(default 03) Non-printable characters in URL rule	*Deny rule disables parameter checks*	
5	●	(default 05) HTTP response splitting rule	(default) None	Edit
6	●	(default 06) Path directory traversal rule	*Deny rule disables parameter checks*	
8	●	(default 08) XSS rule for parameter names	(default) None	Edit
12	●	(default 12) full-/half-width unicode param names	(default) None	Edit

Leading international security solution

Airlock protects Web applications and Web services against attacks and provides sustainable, centrally monitored security. 200 customers in 8 countries already protect over 5000 applications with Airlock.

Ergon delivers specialist IT excellence with a clear focus on customer advantage. The company leads the field in the implementation of customised applications and is an established producer of software products.

ergon
smart people *smart software*

Ergon Informatik AG
Kleinstrasse 15
CH-8008 Zurich

Tel.: +41 44 268 89 00
Fax: +41 44 261 27 50
www.ergon.ch