LOADBALANCER

SECTOR OVERVIEW

A tailored Web Application Firewall (WAF) to protect Metaswitch EAS deployments from attack

Loadbalancer.org, a long-term partner of Metaswitch, has developed a custom WAF solution specifically to meet the security needs of Metaswitch EAS deployments.

Whether deployed as hardware or virtualized, this tailored Loadbalancer.org solution ensures that Metaswitch EAS is highly secure.

Why is having a WAF important: what does it do?

Any web application can be attacked. Web services exposed to the public internet are especially vulnerable, and telecoms services are valuable targets due to the high value attached to a compromised customer account.

A WAF adds a robust layer of protection to any web application by inspecting web traffic in a meaningful way and rejecting traffic that looks malicious. A WAF makes life harder for attackers and prevents web applications from being low-hanging fruit.

What's included in this tailored Metaswitch WAF solution?

Five tailored WAF rules to protect the Metaswitch CommPortal login page

These five custom WAF rules offer enhanced protection for Metaswitch deployments and have been specifically developed to protect the Metaswitch CommPortal login page. They provide:

1. Denial-of-service (DoS) protection
2. Repeated failed login detection and blocking
3. HTTP POST request DoS attack protection
4. Username defense against brute-force attacks on directory numbers
5. Password defense against brute-force attacks

Each rule can be tuned to meet the needs of a specific deployment.

Provisioning service protection rules

Additional custom WAF rules provide protection for Metaswitch SIP provisioning services, including legacy provisioning services where still in use and required.

Brute-force provisioning attacks are mitigated by tracking client connections and blocking abusive IP addresses using custom, Metaswitch-specific rate limiting logic.

Log4j/Log4Shell Defense

Explicit defense against Log4Shell is provided as standard, instantly blocking any requests that resemble an attempt to exploit the Log4j library.

How can I take advantage of this Metaswitch WAF solution?

Site specific protection and flexibility

Site specific rules can also be created to deny and allow clients using a variety of criteria, including:

- Known IP addresses and subnets, for example with block lists and exemptions
- User-Agent request headers, for example blocking scripted attacks
- Geographic location based on IP address.

Prerequisites for an EAS WAF deployment

You must have a fully functional EAS deployment ready for the WAF functionality to be deployed in addition to details of the IP addresses and ports to be used on your network. For full details, refer to the supported preinstallation scenarios in our EAS WAF documentation.

We are not able to assist with the deployment or configuration of Metaswitch servers or infrastructure.

Security customizations for Authenticated Users

Our solution protects the login page of CommPortal, therefore we do not support adding security customizations covering users once they have successfully authenticated and logged into the EAS services.

Extended WAF support for other services and applications

These custom WAF rules are specially designed to protect a Metaswitch EAS deployment. Adding support for additional services and applications is not supported.

Non-standard customizations

Our official EAS WAF documentation outlines all supported and validated customizations. Any general WAF consultancy or log analysis that falls outside the scope of the documentation is not supported. Custom configurations and WAF rules beyond what would be useful to other Metaswitch customers are not supported.

Ongoing updates

You will be eligible to receive any future updates to the custom WAF rule set, which is developed and approved in close partnership with Metaswitch.

Appliance software updates are also included, bringing new features, bug fixes, and prompt patches for security vulnerabilities that arise.

Basic WAF maintenance is included and is covered by our outstanding 24 hour support.

Professional services and training

You only pay for one day of professional services which covers configuring the WAF solution and agreeing upon the baseline security configuration. Training is included and covers monitoring and testing the solution, creating simple site-specific rules, and ensuring services are highly available.

About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.

Contact Support

Email
support@loadbalancer.org

Tel
UK +44 (0)330 380 1064

Support hub
loadbalancer.org/support

Live Chat
loadbalancer.org