metaswitch

A Custom Web Application Firewall (WAF) to Protect Metaswitch EAS Deployments From Attack

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

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

What is included?

Five Core Rules to Protect the CommPortal Login Page

Enhanced protection is provided by five custom WAF rules which have been specifically developed to protect the CommPortal login page. They provide:

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

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

Professional Services and Training

You only pay for one day of professional services which allows for configuring the WAF solution and agreeing upon the baseline security configuration of your system.

Training is included, covering how to monitor and test the solution, creating simple site-specific rules, and ensuring that services are highly available.

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.

Site Specific Protection and Flexibility

Site specific rules can 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

Detailed examples are presented in our EAS WAF documentation and rule set.

loadbalancer.org

What isn't included?

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 pre-installation scenarios in our EAS WAF documentation (pdfs.loadbalancer.org/Metaswitch_EAS_WAF_Gateway_Deployment_Guide.pdf) or speak to our solutions department. 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

The core set of rules is specially designed and tested to protect a Metaswitch EAS deployment. As such, adding any extended WAF support, including for other 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.