Cyber attacks against communications service providers are unfortunately an all too common occurrence. Although Denial of Service (DoS) attacks are particularly prevalent in the telecoms sector, a wide range of different vectors are utilised by attackers.

Metaswitch has seen many different attempts to defraud our customers.

- Brute force attacks on the SIP interface to guess the authentication credentials for subscribers.
- Hacking SIP endpoints to get the authentication credentials stored there.
- Snooping SIP authentication details from configuration files sent from the server to the phone.
- Exploits based around self-care web applications - not even on the voice path.

However, as bad actors are always adapting and evolving their attacks, it is essential that communications service providers remain vigilant and continuously adopt the best practice techniques across all their networks.

For Metaswitch Customers

- Industry standard Web Application Firewall (WAF) provides a default level of protection
- Custom rule set uniquely developed for Metaswitch customers provides unrivaled levels of security
- Additional site specific rule ‘tuning’ available from industry leading support team
- Future-proofing with frequent updates as new threats become known

Obtain Enhanced Protection with a Loadbalancer.org Custom Developed Web Application Firewall (WAF)

Metaswitch solutions have a strong track record of protecting against threats and continue to work hard to help our customers remain secure against the attacks we know today and to pre-emptively secure themselves against the attacks of the future. To enable this, Metaswitch work with and engage the services of a number of specialist partners.

Loadbalancer.org, a long-term partner of Metaswitch, have developed a WAF solution specifically to meet the needs of Metaswitch EAS deployments. Developed collaboratively with Metaswitch and based on real-world customer experience, the Loadbalancer.org solution explicitly addresses known threats in the Metaswitch installed base.

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

Although a wide number of commercial hardware and virtual WAFs are currently available, these are typically not configured to meet the specific and ever-changing threats faced by communication service providers. Therefore, Metaswitch recommend that customers looking to enhance their network security upgrade to a Loadbalancer.org WAF Gateway.
Custom Rule Set Provides Explicit Protection for Metaswitch Customers

The Loadbalancer.org appliance includes a fully integrated industry standard web application Firewall (WAF) but enhanced protection is provided by five custom rules which have been specifically developed to protect a Metaswitch CommPortal environment.

**Rule 1** protects the CommPortal login page against denial-of-service (DoS) attacks. This is accomplished by blocking clients that access the login page more than a set number of times in a given period of time (more than 200 times in 60 seconds by default).

**Rule 2** protects against repeated failed login attempts to CommPortal. It does this by detecting "authentication-Failed" and "retryLimitExceeded" responses from the EAS servers, and blocks clients that accumulate more failed login responses than a set number in a given period of time (more than 20 failed logins in 10 minutes by default).

**Rule 3** protects the CommPortal login page against HTTP POST request-based DoS attacks. Any attempt to sign into CommPortal takes the form of a POST request, so this rule blocks clients that send more than a set number of POST requests in a given period of time (more than 500 POST requests in 10 minutes by default).

**Rule 4** prevents username based abuse. This stops brute-force attacks against specific CommPortal usernames / account numbers, which is achieved by blocking a username after more than a set number of attempted logins using it in a given period of time (more than 20 failed logins in 10 minutes by default).

**Rule 5** prevents password-based abuse. This stops attackers trying to use the same password, such as a common or default password, against a large number of known, or guessable, account numbers. This is done by blocking a password after more than a set number of attempted logins using it in a given period of time (more than 20 failed logins in 10 minutes by default).

Each rule is tuneable to meet the needs of a specific Metaswitch EAS deployment. In busier environments that process significant amounts of traffic, the rules can be relaxed to allow for more requests against the CommPortal login page.

The rules can also be tightened to be more aggressive, which may be appropriate in smaller deployments where only a handful of genuine failed customer logins would be expected over a given period of time.

In addition to the CommPortal specific rules, site-specific rules can be created to block and whitelist clients in a variety of ways. Following the examples in our rule set, it is easy to write rules to block and whitelist clients based on:

- Known IP addresses and subnets, for example blocking IP addresses of known attackers or whitelisting a corporate network
- User-Agent HTTP request headers, for example blocking if the string ‘python’ is detected when attackers are using Python based scripted attacks
- Geographic location based on IP address, for example blocking all connections from outside the country where the deployment is located

The WAF base rule set for Metaswitch EAS is continually being improved, refined and updated to provide extra security as new threats and attacks are encountered in the wild. When used in production, the rules and features outlined here work together to add a robust layer of security to any Metaswitch EAS deployment.