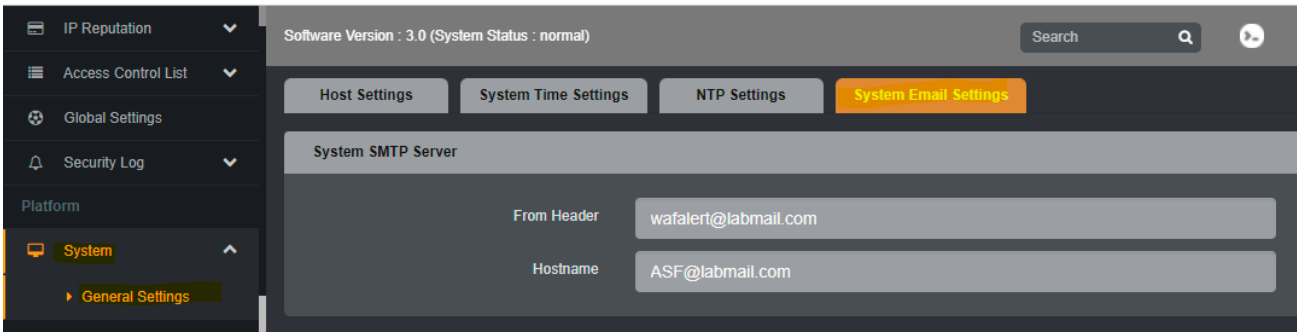
How to create a mail alert for WAF attack events

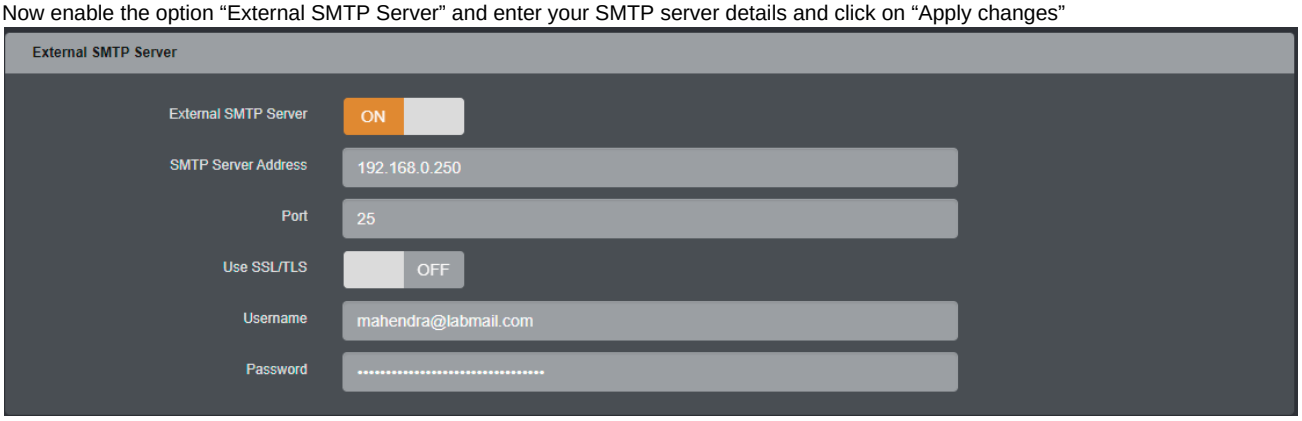
Kindly follow the below steps to create a mail alert for WAF attack events

First we need to configure SMTP mail server details to send a mail alerts from ASF.

1. Login into ASF webui.
2. Expand “System” option and click on “General Settings”.
3. Click on “System Email Settings”.
4. Enter the “From Header” and “Hostname” in “System SMTP Server” and click on “Apply changes”



5. Now enable the option “External SMTP Server” and enter your SMTP server details and click on “Apply changes”

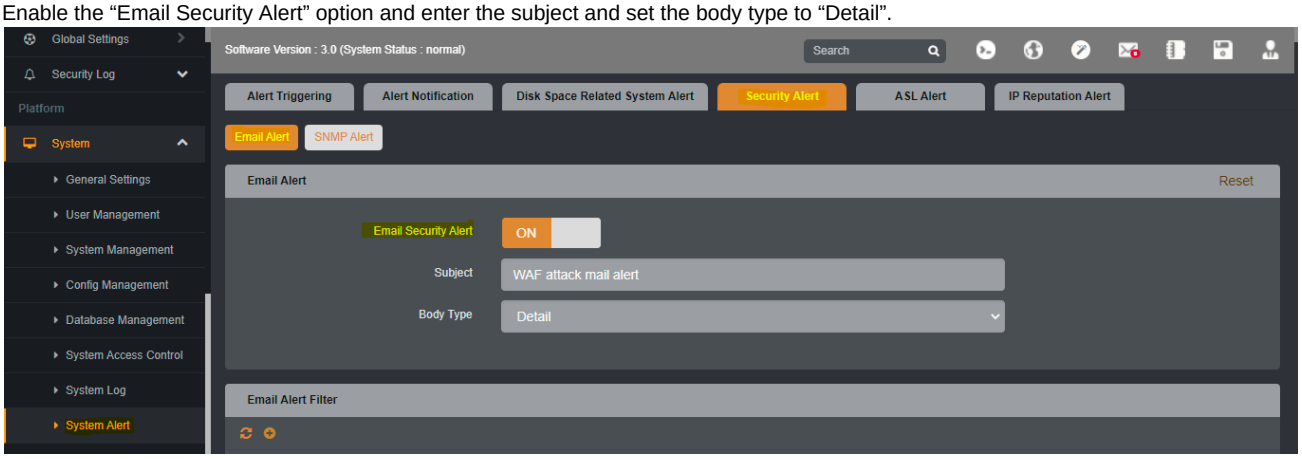


6. Save the configuration.

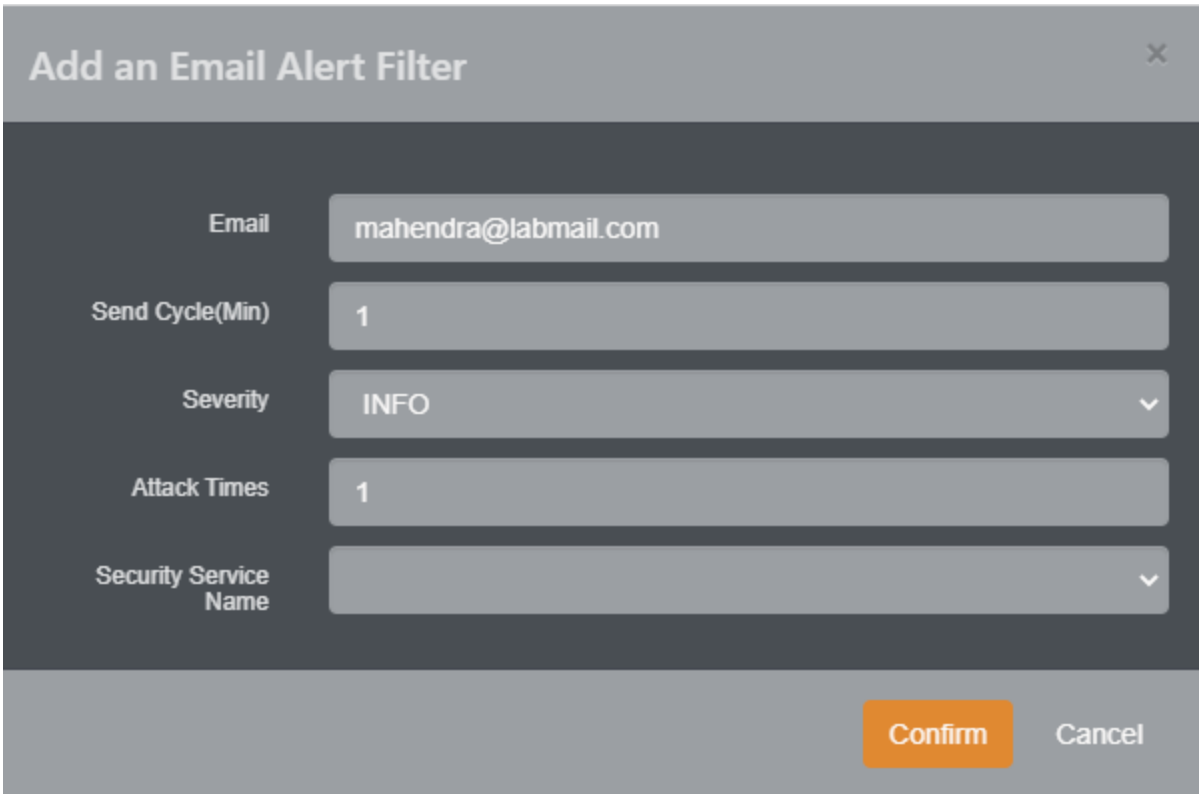
Now we need to configure “security Alert” to send WAF attack mail alert. The system supports a maximum of 3 filter rules.

Kindly follow the below steps for the same.

1. Click on “System Alert” under “System” option.
2. Click on “Email” option under “Security Alert” option.
3. Enable the “Email Security Alert” option and enter the subject and set the body type to “Detail”.



4. Add “Email alert filter” to send the alert mail to respective mail ids.



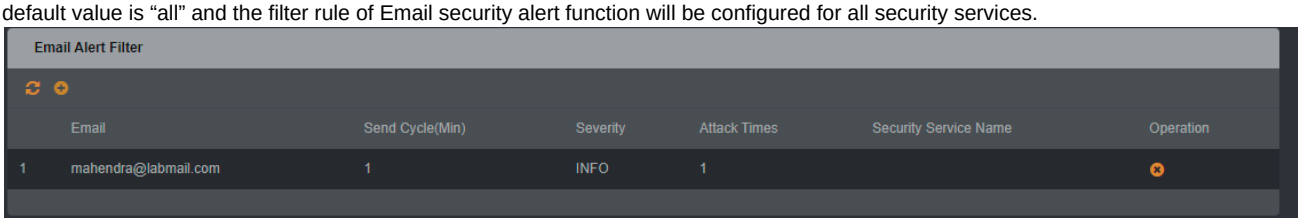
Email_address : This parameter specifies Email address to receive security alert Emails.

Send_cycle : This parameter specifies the interval to detect and send alert Email in minutes. Its value must be an integer ranging from 1 to 10,000.

Severity : This parameter specifies the severity level for attack filtering. Its value must be an integer ranging from 0 (EMERG) to 7 (DEBUG), which represent 7 severity levels: EMERG, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFO or DEBUG.

Threshold : This parameter specifies the threshold of the attack number. Its value must be an integer ranging from the 1 to 2,147,483,647

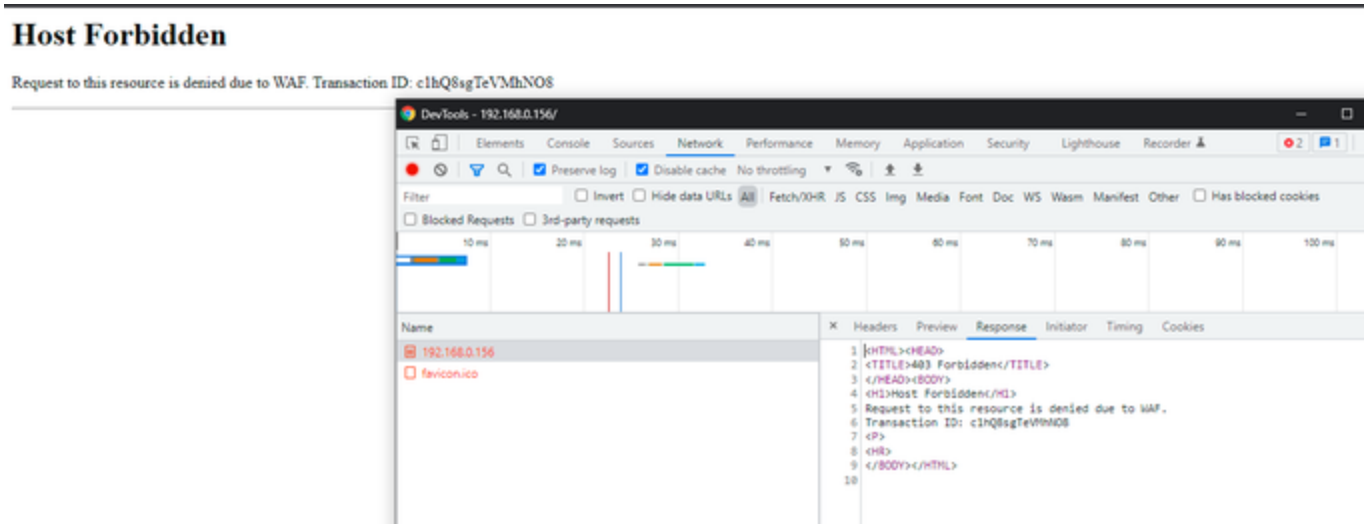
Service_name : This parameter specifies the name of an existing security service. If the “service_name” parameter is not specified, the default value is “all” and the filter rule of Email security alert function will be configured for all security services.



5. Save the configuration.

Now try to send attacks to WAF security service and check if you are able to receive the mail alerts for waf attacks events.

The ASF is able to block the WAF attacks and we can see attack events in WAF logs.



WAF Attack Logs (Filter Condition: Log Count=1000)

Index	Event ID	Date/Time	Severity	Attack Type	Signature ID	Source IP	Security Service Name	Action	URL
52	0.1.2022.2.0.3.0000000026	2022-02-24 21:13:05	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/favicon.ico
51	0.1.2022.2.0.2.0000000024	2022-02-24 21:13:05	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/
50	0.1.2022.2.0.2.0000000023	2022-02-24 21:12:59	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/favicon.ico
49	0.1.2022.2.0.3.0000000025	2022-02-24 21:12:59	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/
48	0.1.2022.2.0.2.0000000022	2022-02-24 21:12:59	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/favicon.ico
47	0.1.2022.2.0.3.0000000024	2022-02-24 21:12:59	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/
46	0.1.2022.2.0.2.0000000021	2022-02-24 21:12:58	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/favicon.ico
45	0.1.2022.2.0.3.0000000023	2022-02-24 21:12:58	WARNING	protocol	800920350	192.168.0.250	VS_CLP	Deny	/

Now check your mail inbox. You will receive the mail alert from ASF as below.