Setting up SSL for Filebeat and Logstash

If you are running Wazuh server and Elastic Stack on separate systems & servers (distributed architecture), then it is important to configure SSL encryption between Filebeat and Logstash. This not applies to single-server architectures.

Note

Many of the commands described below need to be executed with root user privileges.

Generating a self-signed SSL certificate

1. First, we need an SSL certificate and key.

   On the **machine with Logstash server** installed, create a copy of the OpenSSL example configuration file. The file location may vary depending on your operating system:

   a. On Debian or Ubuntu:

   ```
   $ cp /etc/ssl/openssl.cnf custom_openssl.cnf
   ```

   b. On CentOS or Red Hat:

   ```
   $ cp /etc/pki/tls/openssl.cnf custom_openssl.cnf
   ```

   Note

   Typically you will run the Logstash server in your Elastic Stack server or, if you have set up a distributed Elasticsearch cluster, in one of its nodes.

2. Edit the custom configuration file, `custom_openssl.cnf`.

   Find the section `[ v3_ca ]` and add a line like this, including your Elastic server's IP address:

   ```
   [ v3_ca ]
   subjectAltName = IP: YOUR_SERVER_IP
   ```

   For example:

   ```
   [ v3_ca ]
   subjectAltName = IP: 192.168.1.2
   ```

3. Generate the SSL certificate and key:

   ```
   $ openssl req -x509 -batch -nodes -days 3650 -newkey rsa:2048 -keyout /etc/logstash/logstash.key -out /etc/logstash/logstash.crt -config custom_openssl.cnf
   ```

4. You may remove the custom configuration file:

```
$ rm custom_openssl.cnf
```

Configure Logstash server

At this point you should have your SSL certificate and key at `/etc/logstash/logstash.crt` and `/etc/logstash/logstash.key` respectively. Now we'll configure Logstash to use it across with Filebeat.

1. Edit file `/etc/logstash/conf.d/01-wazuh.conf` and uncomment the lines related to SSL under `input/beats`. The active input section should now look like this:

```
input {
    beats {
        port => 5000
        codec => "json_lines"
        ssl => true
        ssl_certificate => "/etc/logstash/logstash.crt"
        ssl_key => "/etc/logstash/logstash.key"
    }
}
```

2. Restart Logstash. The command depends on the OS init system:

a. For Systemd:

```
$ systemctl restart logstash.service
```

b. For legacy SysV Init:

```
$ service logstash restart
```

Configure Filebeat

Now we will configure Filebeat to verify the Logstash server's certificate.

1. On the **machine with Filebeat installed** (Wazuh server), fetch the Logstash server's SSL certificate file at `/etc/logstash/logstash.crt` and copy it into `/etc/filebeat/logstash.crt`.

Here is an **example** you might use to copy the SSL certificate from the Logstash server to Wazuh server where Filebeat is installed:

```
$ scp root@LOGSTASH_SERVER_IP:/etc/logstash/logstash.crt /etc/filebeat
```

2. Edit the file `/etc/filebeat/filebeat.yml` and uncomment the lines related to SSL inside `logstash`. The file should remain like this:

```
output:
 logstash:
   hosts: ["192.168.1.2:5000"]
   ssl:
     certificate_authorities: ["/etc/filebeat/logstash.crt"]
```

3. Restart Filebeat. The command depends on the OS init system:

a. For Systemd:

```
$ systemctl restart filebeat.service
```

b. For legacy SysV Init:

```
$ service filebeat restart
```

Note

More detailed information is available in the Securing communication with Logstash guide from Elastic.