

Why does Search Guard require SSL/TLS?

Jochen Kressin · 2016-07-09



We get a lot of questions like “Why does Search Guard require TLS?” or “Can I run Search Guard without SSL?”.

We officially open the Search Guard blog by explaining the whys behind the decision to make SSL/TLS mandatory. We will post articles regarding Search Guard on a regular basis, so check back often. If you want us to write about a specific topic, just drop us an email or use the comment section below.

tl;dr: In order to secure your data against attacks from the outside and the inside, all traffic must be secured via TLS. Without it, you leave your cluster open for attacks.

We understand that if you have no prior knowledge about TLS, getting the concepts behind it can be confusing. You need to deal with certificates, certificate authorities, key- and truststores and so on. But on the other hand, data security will always be a topic that comes at a price. We believe that you should familiarize yourself with security technologies such as TLS, so you know exactly what is happening in the background to secure your data.

So, let's jump right in and talk about some of the comments we received (as always, thanks very much for your feedback folks!):

“I just want to test Search Guard quickly and don’t want to be bothered with TLS.”

If you just want to test drive Search Guard, or set up a PoC, you do not have to deal with the TLS layer of Search Guard.

update: The Search Guard Bundle has been replaced by our [Search Guard Demo Installer](#) see the [documentation](#) to learn more.

We provide an Elasticsearch installation pre-configured with Search Guard and Search Guard SSL, uncreatively called “Search Guard Bundle”. You just need to download, unzip and start. The bundle comes with the enterprise features as well, so you can test all of them. The sgadmin CLI (to update the configuration) is also pre-configured with the correct command line settings. The only thing you need to do is update the configuration files, and run sgadmin.sh.

If you want to dig a little bit deeper into TLS, you can also use our [example PKI scripts](#) that ship with Search Guard SSL. The scripts generate all required certificates for a 3-node cluster.

Last but not least: We’re also planning to ship Search Guard with demo certificates in future.

“I do not need inter-node encryption.”

If the traffic between the nodes is not encrypted, anyone with access to your network can easily spy on your data. And, furthermore, also modify it. So, without SSL you leave yourself vulnerable for those kinds of attacks. However, there is another very important reason to use TLS, and that is that TLS is much more than just encryption:

When talking about SSL/TLS, most people immediately think about HTTPS and that it is used for encrypting sensitive data, such as username and password on a login page. If the data is encrypted, no one can see it in clear text, and everything is fine.

Right? No, unfortunately not. Encrypting data alone is not enough to secure the communication between two systems. You also need to make sure that the system you are talking to is indeed the correct one, and not a malicious attacker impersonating it. In other words, the other system has to prove its identity to you before you send any data, and that is exactly what TLS provides.

Can I see your ID please?

During the first steps of the SSL handshake protocol, the server sends its certificate to the client. The client verifies the certificate, and thus the identity of the server. If this verification fails, the handshake is aborted. If it succeeds you can be pretty sure that the server you are talking to is indeed the one it claims to be.

While it is common that only the server has to prove its identity to the client, TLS is not limited to that. The server can also request a certificate from the client and check the clients identity. This is called “Client Authentication”, and is supported (but not mandatory) by Search Guard.

To sum it up, TLS you can make sure that:

- The data cannot be sniffed

- The data can not be modified
- Only trusted clients or nodes can interact with the cluster

In fact, if you do not need advanced authentication/authorization, and just need to make sure that only trusted parties can query, update or delete data, TLS is all you need. Some users therefore only install the Search Guard SSL plugin, because they do not need all the other features.

“My cluster runs in a private, secure network, I do not need SSL.”

When we talk about hackers attacking networks to steal data, most of us have this picture in mind: Someone on the other side of the globe sits in a dark room, only lit by three monitors that this person is watching simultaneously, while typing on the keyboard with lightning speed.

55% of all attacks come from the inside

But the truth is, less than half of all attacks come from outside your network. The other attacks actually occur from the inside. It could be one of your employees, contract workers or even vendors or business partners. An IBM study shows that 60% of all attacks come from “anyone who has physical or remote access to a company’s assets”:

IBM Security Study

More resources about inside threats:

<http://www.cnet.com/news/the-biggest-cyber-threat-to-companies-could-come-from-the-inside/>
<http://www.cio.com/article/2985790/security/are-your-biggest-security-threats-on-the-inside.html>
<https://hbr.org/2014/09/the-danger-from-within>

“My cluster runs behind nginx which does SSL already.”

Yes, but this only makes sure that the traffic to and from your webserver is secure. Everything behind it is unprotected and thus insecure. Again, any attacker that has access to your network would be able to steal your data.

Getting security right

Getting security right can be complex and requires an effort. We believe it’s better to familiarise yourself with the concepts behind SSL/TLS than to leave you with a half-baked solution that leads you to believe your data is secure.

Note: We realize TLS is not the silver bullet for security, and has some flaws of its own. However, at the time of writing, we think that TLS is best suited for the purpose of Search Guard.

Image source: Tashatuvango/Shutterstock

This article was published on the Search Guard blog: <https://search-guard.com/blog/search-guard-ssl-tls/>
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · [Start a free trial](#)