Zero-trusted networks

Cliff Staley · 2019-01-02

Zero trusted networks

The security level can be increased endlessly. It is crucial to choose the best possible tradeoff between the expenses and the risks. What is *zero-trust* and is it worth it? According to Gartner, *zero-trust posture* is No. 4 of top 10 security projects one should focus in 2018. In this post, we present zero trusted networks and its motivations.

Firewall and VPN are not enough

Firewall and VPN are perimeter protection layer that separate your organisation's resources from the internet. They protect from several risks, but once there is a hole in a perimeter, they do not protect you from anything. It is like a flood bank - even if a tiny part is broken, the rest is useless.

Well, the flood banks are still useful and popular nowadays, aren't they? Yes, they are. The difference is that, when compared to firewalls, they are much easier to maintain as one can measure their height, density and see if they surround all the area to protect. On the other hand, a firewall is a set of rules based on IP addresses and server ports. The rules contain tons of exceptions to meet business requirements as one cannot reject all the traffic. Humans create the rules but no human can control all the rules established, which makes it error-prone.

Moreover, once a port is opened, one can barely filter data that is transferred. In other words, if a host can connect to an unsecured Elasticsearch cluster, anything requested from that host can be done with

© 2026 floragunn GmbH · search-guard.com

the cluster and its data.

The problem with VPN is that several actors are allowed to connect. For example, a student intern, a guests at your office or an employee that took home office and decided to work at the coffee shop. VPN protects from actors outside the private network, but the network already contains several actors that one cannot trust.

According to forbes.com, 58% of healthcare breaches are initiated by the insiders. Another Intel report presents that insiders are responsible for 43% of data loss. Half of them were done intentionally while others accidentally. If you rely on a firewall (or a proxy) and allow requests to search the Elasticsearch index, you also allow requests that can damage the data.

To sum it up: Perimeter security is helpful, but it is not enough.

Security at the application layer

Security cannot be achieved without being implemented at the application layer. It is the application layer that is aware of a user's context and permissions. A firewall or a proxy does not know what indices are allowed to be read by users. It only knows a host name and a port 9200. It can allow or ban the traffic but this is not the level of granularity that is needed.

Can we trust a request from a host within our private network? We can trust it that much as we trust the firewall and a VPN. But we cannot rely on them. It is much clearer to say we cannot trust such requests, which leads us to zero-trusted networks.

> Always assume that the attacker is already in your network

In practice, this means that:

- All the traffic *client to server* and *server to server* has to be secured by TLS.
- Traffic has to be encrypted all the time. It is not allowed to send any data in cleartext over the network.

Search Guard and zero trusted networks

Zero trusted networks specify clear requirements for Elasticsearch clusters:

- Authorisation has to be done directly on the cluster. Any other solution (VPN, firewall or proxy) is a perimeter security that cannot filter malicious requests reliably.
- The traffic between the cluster nodes needs to be encrypted. Zero trust means we cannot trust the node to node network connection.

Fortunately, Search Guard meets all the zero-trusted network requirements. Moreover, all of them are met since the first version of our product. These requirements have been driving the architecture of our system and its codebase.

Further read

- Why perimeter security is dead (presentation)

© 2026 floragunn GmbH · search-guard.com

Sources:

- https://www.networkworld.com/article/3307118/network-security/zero-trust-networking-ztn-don-t-trust-anything.html
- https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html
- https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/
- https://www.forbes.com/sites/louiscolumbus/2018/08/31/58-of-all-healthcare-breaches-are-initiated-by-insiders/#52137091601a
- https://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/

Image: shutterstock / Alexandra_F

This article was published on the Search Guard blog: https://search-guard.com/blog/elasticsearch-zero-trusted-networks/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial