(https://help.zscaler.com)

About the Zscaler Cloud Architecture

Search

Zscaler operates the world's largest security-as-a-service (SaaS) cloud platform to provide the industry's only 100% cloud-delivered web and mobile security solution. The Zscaler highly scalable, global multi-cloud infrastructure features three key components: the Zscaler Central Authority, Zscaler Enforcement Nodes, and Nanolog clusters.

Zscaler Central Authority

The Zscaler Central Authority (CA) is the brain and nervous system of a Zscaler cloud. It monitors the cloud and provides a central location for software and database updates, policy and configuration settings, and threat intelligence. The CA consists of one active server and two servers in passive standby mode. The active CA replicates data in real time to the two standby CAs, so any of them can become active at any time. Each server is hosted in a separate location to ensure fault tolerance.

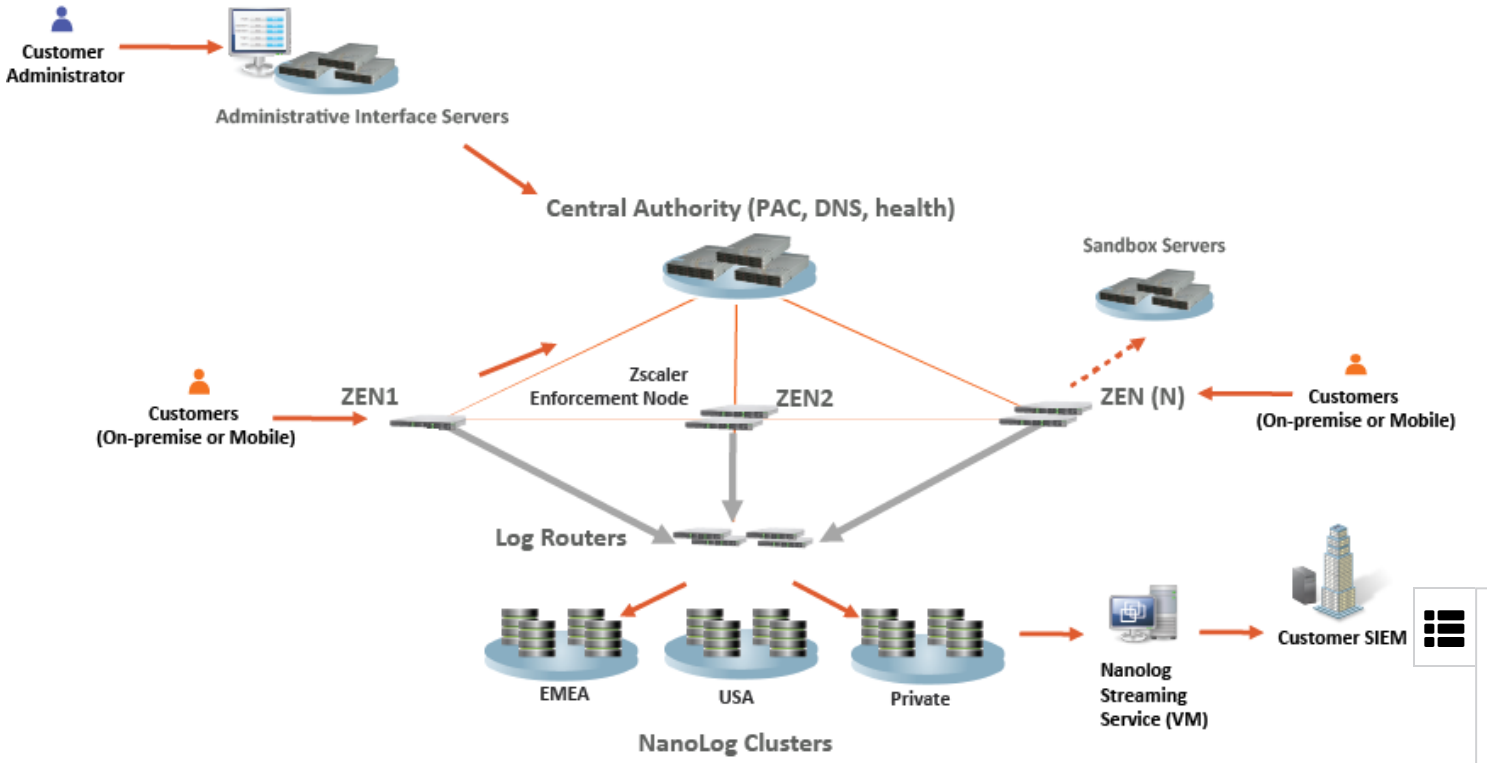
Zscaler Enforcement Nodes

Zscaler Enforcement Nodes (ZENs) are full-featured, inline Internet security gateways that inspect all Internet traffic bi-directionally for malware, and enforce security and compliance policies. An organization can forward its traffic to any ZEN in the world or use the advanced geo-IP resolution capability of Zscaler to direct its users' traffic to the nearest ZEN. When the user moves to a different location, the policy follows the user, with the ZEN downloading the appropriate policy. Each ZEN can handle hundreds of thousands of concurrent users with millions of concurrent sessions. With the exception of

sandboxing, all inspection engines run within the ZEN. Customer traffic is not passed to any other component within the Zscaler infrastructure. The TCP stack on the ZEN runs in user mode, and is specially crafted to ensure multitenancy and data security. ZENs never store any data to disk. Packet data is held in memory for inspection and then, based on policy, is either forwarded or dropped. Log data generated for every transaction is compressed, tokenized, and exported over secure TLS connections to Log Routers that direct the logs to the Nanolog cluster, hosted in the appropriate geographical region, for each organization. ZENs are always deployed in active-active load balancing mode all over the world, and the CA monitors the health of ZENs to ensure availability.

Nanolog clusters

Nanolog clusters store transaction logs and provide reports. Each cluster consists of one active server and two servers in passive standby mode. The active Nanolog immediately replicates data to the other two servers, so any of them can become active at any time, with no data loss. Each Nanolog server is hosted in a separate location to ensure fault tolerance. Every second, a Nanolog cluster receives logs from all over the world, correlates them to a specific customer organization, and writes them to disk for high-speed retrieval of reporting and analytics. A Nanolog cluster processes up to 12+ billion logs per day. Additionally, Zscaler offers a Nanolog Streaming Service (NSS), which uses a virtual appliance to stream web and firewall traffic logs in real time from the Zscaler Nanolog to the customer's security information and event management (SIEM) system.



Additionally, each cloud has various support systems and servers, including:

- Sandbox servers, where files selected for behavioral analysis are sent for analysis and reports are stored.
  For more information, see How do I view Sandbox reports and data? (https://help.zscaler.com/zia/how-do-i-view-sandbox-reports-and-data)
- PAC file servers, which host Zscaler PAC files and custom PAC files uploaded to Zscaler. Configuring browsers to use PAC files is one of the traffic forwarding methods that Zscaler supports.
  To learn more, see About Hosted PAC Files (https://help.zscaler.com/zia/about-hosted-pac-files).
- Administrative interface servers, which provide an intuitive, multi-tenant interface for policy management and reporting.
- Log Routers, which ensure logs for each organization are stored in the appropriate Nanolog cluster.

All components communicate with each other over an encrypted SSL tunnel.

Finally, Zscaler Feed Central is a separate Zscaler cloud that is used solely for the centralized distribution of various feeds to the Zscaler clouds. Zscaler has a number of partnerships with Microsoft, Google, RSA, Verisign, and others for getting data feeds,

including feeds for URL filtering, anti-virus definitions, and IP reputation. Zscaler Feed Central distributes its threat intelligence and other feeds to the CA, which then sends updates to the ZENs, ensuring that every ZEN has the latest version of the URL database and the latest malware and threat information.

> An organization is provisioned on one cloud and its traffic is processed by that cloud only. The name of the cloud on which an organization is provisioned is specified in the administrative URL that the customer admin uses to log in to Zscaler. To learn how to find your cloud name, see What is my cloud name? (https://help.zscaler.com/zia/what-my-cloud-name)