Exalate Cloud - Whitelist

Last Modified on 12/20/2022 3:28 am EST

You tried to access the Exalate cloud gateway, which is the entry address for Exalate Cloud.
If you need to whitelist the Exalate cloud - all Exalate cloud hosts send a PTR record to **whitelist.exalate.cloud**

PTR Records - Whenever applying a reverse DNS lookup on an incoming IP, it will return whitelist.exalate.cloud. This approach allows whitelisting the Exalate hosts.

When configuring **whitelist.exalate.cloud** on the firewall, the firewall will be able to validate that incoming TCP connections are coming from one of the exalate nodes by doing a reverse DNS lookup of the source IP.

Why is there no fixed IP list?

Every exalate node is dedicated to a single tracker (such as ServiceNow, or Jira ...)
This single-tenant architecture is essential for guaranteeing information security. The outgoing connections (from an exalate node) are direct (and not routed over a proxy)

Exalate nodes are hosted on Google cloud, and the number of machines required to host all the nodes is growing exponentially. Furthermore, whenever a host is patched (or restarted), all nodes on that host will move to another host. The consequence is that the IP address of the exalate node will change (it is not fixed) and the set of IP addresses (which the node can have), is also changing.

The PTR approach is a common technology to validate the source IP addresses and will require a lot less maintenance than the configuration of fixed ips

Product
About Us
Release History
Glossary
API Reference
Security
Pricing and Licensing
Resources
Academy
Blog
YouTube Channel
Ebooks
Still need help?
Join our Community
Visit our Service Desk
Find a Partner