Cloud Threat Intelligence

One of the best features of ZenArmor, is it's real-time Cloud Reputation and Threat Intelligence. These features are served through what they call ZenArmor Cloud, which is hosted by them, using a Google Cloud Infrastructure. ZenArmor Cloud is essentially a database that is continuously updated as new threats become realized. It allows for real time security threat intelligence, web site categorization, and site reputation/ranking which can be used for whitelisting or blacklisting.

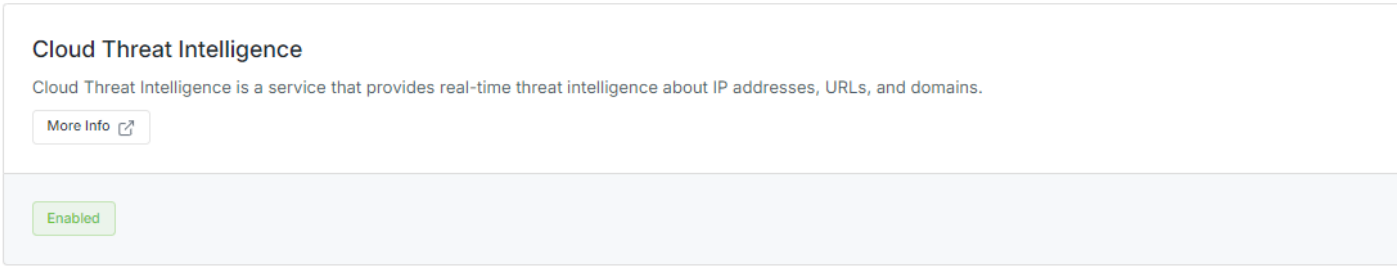
ZenArmor sources it's data from their own database, their SOC, commercial threat intelligence feeds and public known threat databases, and several more reliable entities. With this large quantity of information, their AI-based threat intelligence can protect your network and devices from a large variety of attacks.

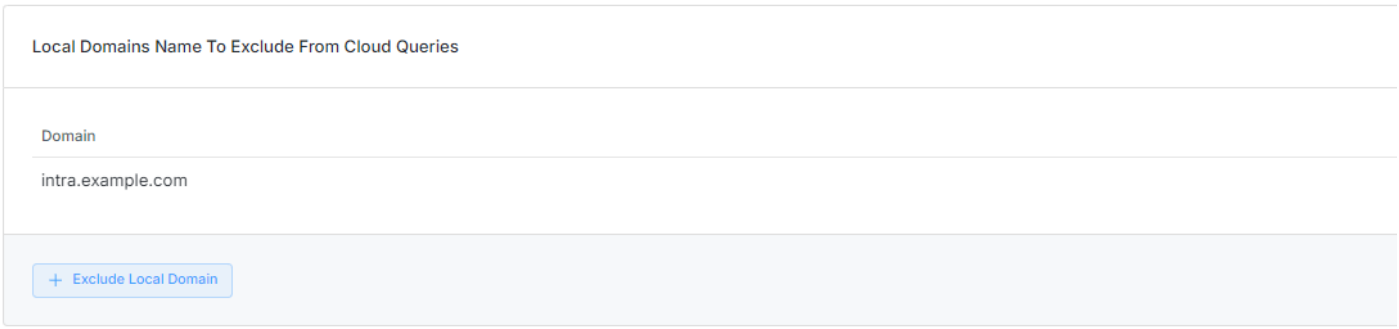
How it Works

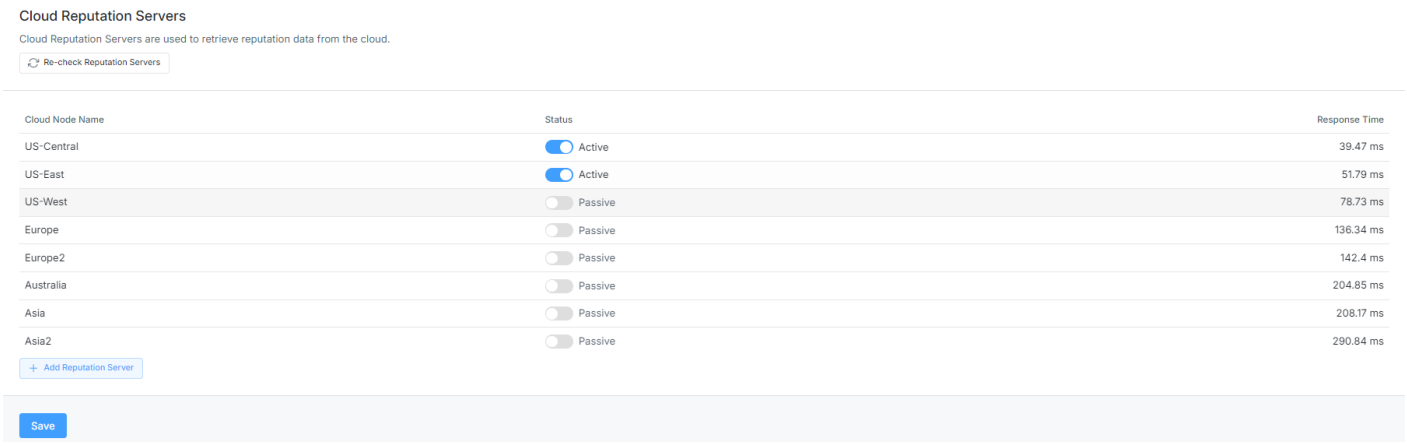
Whenever a device within a protected network attempts to start a connection, the cloud data is queried in real time. The ZenArmor packet engine will process the flow and query the data from the nearest cloud server. Then, it will decide whether the connection is secure and decides how to proceed based on the policies and rules you have set up. As stated in their documentation, all communication between the packet engine and the cloud server uses proprietary encryption on UDP ports 5355 and 5356.

Configurations

You can configure Cloud Threat Intelligence via OPNsense Web GUI or Zenconsole. You can clear Cloud cache, exclude local domains, and also select their cloud servers that are closest to you to improve speed of connections and queries.







Revision #2
Created 17 March 2024 07:28:05 by Austin
Updated 17 March 2024 20:11:35 by Austin