# #

Sentry Nodes

Validators are responsible for ensuring that the network can sustain denial of service attacks.

One recommended way to mitigate these risks is for validators to carefully structure their network topology in a so-called sentry node architecture.

Validator nodes should only connect to full-nodes they trust because they operate them themselves or are run by other validators they know socially. A validator node will typically run in a data center. Most data centers provide direct links the networks of major cloud providers. The validator can use those links to connect to sentry nodes in the cloud. This shifts the burden of denial-of-service from the validator's node directly to its sentry nodes, and may require new sentry nodes be spun up or activated to mitigate attacks on existing ones.

Sentry nodes can be quickly spun up or change their IP addresses. Because the links to the sentry nodes are in private IP space, an internet based attacked cannot disturb them directly. This will ensure validator block proposals and votes always make it to the rest of the network.

To setup your sentry node architecture you can follow the instructions below:

Validators nodes should edit their config.toml:

Comma separated list of nodes to keep persistent connections to

Do not add private peers to this list if you don't want them advertised

persistent_peers= [list of sentry nodes]

Set true to enable the peer-exchange reactor

pex= false Sentry Nodes should edit their config.toml:

Comma separated list of peer IDs to keep private (will not be gossiped to other peers)

Example ID: 3e16af0cead27979e1fc3dac57d03df3c7a77acc@3.87.179.235:26656

private_peer_ids= "node_ids_of_private_peers"