Implement security practices

Each validator candidate is encouraged to run its operations independently. Diversity across individual setups increases the resilience of the network.

Manage Digital Keys with HSM

Key management is mission-critical for validators. If an attacker gains access to a validator's private key, it puts the validator's entire delegated stake at risk. Hardware Security Modules (HSMs) are an important strategy for mitigating this risk. You may also want to consider using Horcrux, a multi-party-computation (MPC) signing service.

Note that Horcrux may impact your signing performance, so it's recommended to test it in Testnet

Defend Against DDoS Attacks

Validators are responsible for ensuring that the network can defend against denial-of-service (DDoS) attacks. Validators can mitigate these attacks by carefully structuring their network topology in a sentry node architecture. Validator nodes should only connect to full nodes that they trust. These nodes can be run by the same validator or other validators that they know.

A validator node will typically run in a data center, and most data centers provide direct links to major cloud providers. A validator can use these 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. This may require new sentry nodes to be spun up or activated to mitigate attacks on existing ones. Sentry nodes can be quickly spun up or used to change IP addresses. Because links to the sentry nodes are in private IP space, an internet-based attack cannot directly disturb them. This will ensure a validator's block proposals and votes always make it to the rest of the network.

Learn more about sentry-node architecture.

For Validator Nodes

- Edit theconfig.toml
- file:

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

"comma separated list of sentry node addresses"

Set to true to enable the peer-exchange reactor.

pex

false

For Sentry Nodes

- Edit the 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

"validator node address"

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

private_peer_ids

"nodeid of the validator" A node address has the following format: nodeid@ip:port. You can get the node id by running seid tendermint show-node-id. The default port is 26656.

Update minimum gas prices

- Open~/.sei/config/app.toml
- Modifyminimum-gas-prices
- and set the minimum price of gas a validator will accept to validate a transaction and prevent spam.

Last updated onMay 23, 2024 Register a Validator Restore a Validator