哨兵节点

验证节点需要确保网络能够承受分布式拒绝服务 (DDoS) 攻击。

减轻此类风险的推荐方法是使用 Sentry 节点构建可以保护验证节点的网络拓扑。

验证节点只能连接到他们信任的完整节点，例如自己维护的完整节点或社区中已知的其他验证者运行的节点。验证节点通常在数据中心运行。大多数数据中心提供直接连接到云服务提供商的网络。验证节点可以通过这样的网络连接到云上的哨兵节点。这将 DDoS 攻击的负担直接从验证节点转移到其 Sentry 节点，并且可能需要在必要时启动或激活新的 Sentry 节点以减少此类攻击的影响。

Sentry 节点可以快速启动或更改其 IP 地址。由于验证节点和哨兵节点之间的链路在私有 IP 网络中，黑客无法通过网络直接攻击验证节点。这将确保区块提议和验证节点的投票将始终由 Sentry 节点正常广播。

要配置 Sentry 节点架构，您可以按照以下说明进行操作：

验证节点应该编辑他们的 config.toml：

```
# Comma separated list of nodes to keep persistent connections
# Do not add private peers to this list if you do not want them advertised
persistent_peers = [list of sentry nodes]

# Set true to enable the peer-exchange reactorpex = false
```

Sentry 节点应该编辑它们的 config.toml：

```
# comma separated list of peer IDs to keep private (will not be gossiped to other peers)
# Example ID: 3e16af0cead27979e1fc3dac57d03df3c7a77acc
private_peer_ids = "node_ids_of_private_peers"
```

参考文档：https://forum.cosmos.network/t/sentry-node-architecture-overview/454