Stateful Packet Inspection

Contents

What is Stateful Packet Inspection?

Stateful Packet Inspection (SPI) is a firewall technology that monitors the state of active connections and inspects the packets flowing through a network to enforce security policies. Unlike traditional packet filtering, which examines individual packets based on predefined rules, SPI keeps track of the state of network connections and makes decisions based on the context of those connections.

How does it work?

1. Tracks Connections: Monitors active connections in a state table. This table stores information about each connection, including source and destination IP addresses, source and destination ports, and the current state of the connection (e.g., established, related, new).

2. Evaluates Packets: Compares packets against predefined rules.

3. Context-Aware Inspection: Examines packets based on connection state.

4. Dynamic Security: Adapts rules based on connection status.

Is it available in Teltonika RUTOS?

Yes, SPI is enabled by default in Teltonika RUTOS.

How to check the current connection state in Teltonika RUTOS?

1. In WebUI, Go to **Status > Realtime Data > Connections**.

2. In CLI, use the below command to show the iptables rules involving “State Module”.

```
iptables -L -n -v | grep "state"
```

3. In CLI, use the command **cat /proc/net/nf_conntrack** to display the connection tracking table maintained by the kernel. It shows active connections and their states, which is essential for SPI.

When would you need to bypass SPI and how?

Disabling the SPI would not be recommended as they play a crucial role in network security by tracking the state of connections and helping to prevent various types of attacks. But in certain scenarios you might be required to disable or bypass it, like.

1. Compatibility with certain protocols or applications.

2. Troubleshooting Network connectivity issues.

3. Specialised Network configuration.

To bypass connection tracking you can add a rule like

```
iptables -t raw -A PREROUTING -i interfaceName -p tcp --dport destinationPort
-j CT --notrack
```