

Inspection of MPLS Traffic Overview

Multiprotocol Label Switching (MPLS) is an IP label switching technology that enables predetermined paths to specific destinations, called Label Switched Paths (LSPs), to be established through an inherently connectionless IP network. In MPLS networks, packets contain short labels that describe how to forward them through the network.

With MPLS decapsulation enabled, the IDP engine can inspect the IPv4 payload and pass through non-IPv4 payload. Note the following requirements and limitations:

- The IDP engine cannot decapsulate other encapsulated protocols within an MPLS frame. For example, the IDP engine cannot decapsulate the MPLS frame, find a GRE frame, decapsulate the GRE, and inspect the payload. Instead, the IDP engine passes through such traffic.
- If your traffic uses Ethernet frames larger than 1750 bytes, you must ensure the IDP default maximum frame size is sufficient (the default maximum frame size is 9014 bytes). In addition, we recommend you set the maximum transmission unit (MTU) on the switch or router connected to the IDP appliance to 1750 bytes or lower.

The IDP appliance does not participate in Label Distribution Protocol (LDP). When the IDP appliance receives the traffic, the IDP engine stores the MPLS label stacks of client-to-server or server-to-client directions. After processing the flow, the IDP appliance forwards the IP frames with the label stack it had stored when it created the flow, relying on the label switch router (LSR) to add the correct MPLS labels to the packet.

In some cases, the IDP engine is programmed to act in the server-to-client direction before it has seen and stored a server-to-client MPLS label. In effect, these connections are dropped. You might observe dropped MPLS traffic if the following rule elements apply:

- IDP rulebase – Action: Close Client (limitation applies to VLAN tagged traffic only)
- IDP rulebase – IP action: IP Close
- SYN Protector rulebase – Relay mode
- Network Honeygot rulebase – Impersonate mode

MPLS support is not enabled by default. You can use the CLI to enable MPLS support.

Related Topics The following related topic is included in the *IDP Administration Guide*:

- Enabling Inspection of MPLS Traffic