Stream UDP Inspector

Stream UDP Inspector Overview

Type	Inspector (stream)
Usage	Inspect
Instance type	Multiton
Other Inspectors Required	None
Enabled	`true`

User Datagram Protocol (UDP) is a connectionless, low-latency transport layer protocol. UDP enables stateless communication between two network endpoints before an agreement is provided by the receiving party. To evaluate the integrity of the message header and data, UDP uses checksums.

The `stream_udp` inspector checks the source and destination IP address fields in the IP datagram header, and the port fields in the UDP header to determine the direction of flow and identify a session. A session ends when a configurable timer is exceeded, or when either endpoint receives an ICMP message that the other endpoint is unreachable.

The UDP stream inspector does not generate events. You can enable packet decoder rules (GID 116) to detect UDP header anomalies.

Best Practices for Configuring the Stream UDP Inspector

Consider the following best practices when you configure the `stream_udp` inspector:

- Create a `stream_udp` inspector for each session timeout that you want to apply to a host or endpoint. The stream UDP inspector associates the `session_timeout` with the UDP hosts defined in the `binder` inspector.

You can have multiple versions of the `stream_udp` inspector in the same network analysis policy.

- Enable packet decoder rules (GID 116) to detect UDP header anomalies.

Stream UDP Inspector Parameters

session_timeout

Specifies the number of seconds that the UDP inspector keeps an inactive UDP stream in the state table. The next time Snort detects a UDP datagram with the same flow key, it checks if the session timeout on the earlier flow has expired. If the timeout has expired, Snort closes the flow and starts a new flow. Snort checks for stale flows associated with the base stream configuration.

Type: integer

Valid range: `0` to `2,147,483,647 (max31)`

Default value: `30`

Stream UDP Inspector Rules

The `stream_udp` inspector does not have any associated rules.

Stream UDP Inspector Intrusion Rule Options

The `stream_udp` inspector does not have any intrusion rule options.