Stream ICMP Inspector

Stream ICMP Inspector Overview

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

Internet Control Message Protocol (ICMP) is a network-layer protocol used by network utility applications and network devices. ICMP sends diagnostic and error information to identify communication success or failure between IP hosts. An ICMP message includes header and data sections.

ICMP conveys information about other flows. It does not carry data that needs reassembly, nor does it require target-based binding.

The `stream_icmp` inspector defines ICMP flow tracking. For pings, the inspector provides basic flow tracking through the source and destination IP address fields and the port fields in the ICMP header. For unreachable destinations, the inspector analyzes the original IP addresses and transport ports, then it updates the session's state. The `port_scan` inspector can use the unreachable host and port, if available.

Best Practices for Configuring the Stream ICMP Inspector

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

- Create a `stream_icmp` inspector for each session timeout that you want to apply to a host or network. The `stream_icmp` inspector associates the `session_timeout` with the ICMP hosts or networks defined in the `binder` inspector.

  You can have multiple versions of the `stream_icmp` inspector in the same network analysis policy (NAP).

Stream ICMP Inspector Parameters

session_timeout

Specifies the number of seconds that the `stream_icmp` inspector keeps an inactive ICMP stream in the state table. The next time Snort detects an ICMP 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: `60`

Stream ICMP Inspector Rules

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

Stream ICMP Inspector Intrusion Rule Options

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