Stream IP Inspector

Stream IP Inspector Overview

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

Internet Protocol (IP) is a connectionless, network-layer protocol that forms the basis of the internet. IP uses host addresses to route messages from a source host to a destination host across IP networks. IP can route both TCP and UDP data packets in addition to other transport protocols.

An IP message contains header and data sections. The IP header includes IP addresses used to route a messsage to its destination. The IP data section encapsulates the message payload. IP handles reassembly and fragmentation of messages.

The `stream_ip` inspector detects an IP network flow and examines the packets in the flow. The `stream_ip` inspector defines IP session and flow tracking, operating system policy, and datagram overlaps configuration parameters. Depending on the mode, either the `stream_ip` inspector or the Snort data plane handles defragmentation.

Best Practices for Configuring the Stream IP Inspector

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

- Create a `stream_ip` inspector for each IP configuration that you want to apply to a host, endpoint, or network. The stream IP inspector associates the IP configuration with the IP hosts, endpoints, or networks defined in the `binder` inspector.

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

Stream IP Inspector Parameters

max_overlaps

Specifies the maximum allowed overlaps for each datagram. Specify `0` to permit an unlimited number of overlaps.

You can enable rule 123:12 to trigger an alert for excessive fragment overlaps.

Type: integer

Valid range: `0` to `4,294,967,295 (max32)`

Default value: 0

min_frag_length

Specifies the minimun number of bytes expected in the IP fragment. Specify `0` to permit an unlimited number of bytes in the IP fragment.

You can enable rule 123:13 to trigger an alert for fragments shorter than `min_frag_length`.

Type: integer

Valid range: `0` to `65535`

Default value: 0

min_ttl

Specifies a minimum number of hops or time to live (TTL). Discard fragments below the specified minimum TTL.

You can enable rule 123:11 to trigger an alert for fragments with a TTL below this value.

Type: integer

Valid range: `1` to `255`

Default value: `1`

policy

Specifies the operating system of the target host or hosts. The operating system determines the appropriate IP fragment reassembly policy and operating system characteristics. You can define only one `policy` parameter for each stream IP inspector.

Note If you set the `policy` parameter to `first`, Snort may provide some protection, but miss attacks. You should edit the `policy` parameter of the IP stream inspector to specify the correct operating system.

Type: enum

Valid values: Set a type of operating system for the `policy` parameter.

Table 1: Valid Values for Policy

Policy	Operating Systems
`first`	Unknown OS
`linux`	Linux
`bsd`	AIX FreeBSD OpenBSD
`bsd_right`	HP JetDirect (printer)
`last`	Cisco IOS
`windows`	Windows 98 Windows NT Windows 2000 Windows XP
`solaris`	Solaris OS SunOS

Default value: `linux`

session_timeout

Specifies the number of seconds that the `stream_ip` inspector keeps an inactive IP stream in the state table. The next time Snort detects an IP 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 IP Inspector Rules

Enable the `stream_ip` inspector rules to generate events and, in an inline deployment, drop offending packets.

Table 2: Stream IP Inspector Rules

GID:SID	Rule Message
123:1	inconsistent IP options on fragmented packets
123:2	teardrop attack
123:3	short fragment, possible DOS attempt
123:4	fragment packet ends after defragmented packet
123:5	zero-byte fragment packet
123:6	bad fragment size, packet size is negative
123:7	bad fragment size, packet size is greater than 65536
123:8	fragmentation overlap
123:11	TTL value less than configured minimum, not using for reassembly
123:12	excessive fragment overlap
123:13	tiny fragment

Stream IP Inspector Intrusion Rule Options

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