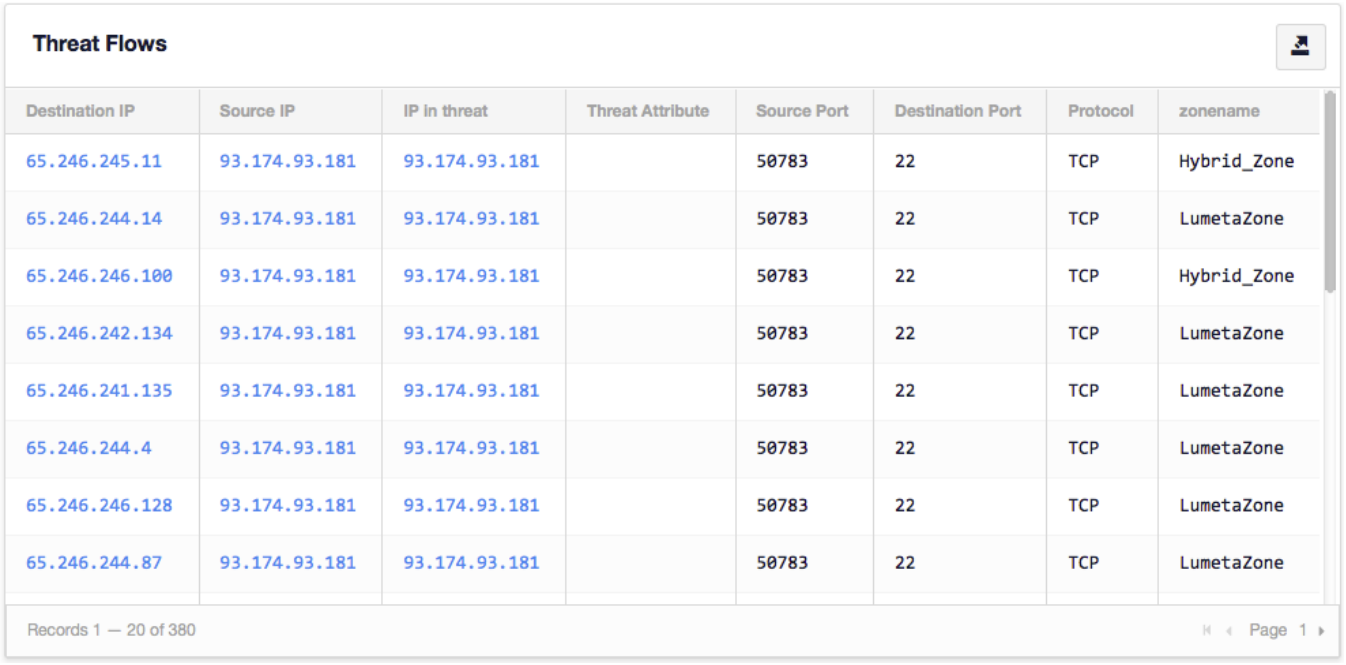
iDefense

iDefense is a closed-source threat intelligence feed available to all Asset Manager customers. This feed correlates iDefense IPs against your network's IPs to produce actionable lists of zombie devices and threat flows in your network.

To use iDefense, you'll need to obtain an iDefense license key (not provided by FireMon).

To produce threat flow results, you'll need a single source of NetFlow data such as Gigamon NetFlow. Asset Manager can receive NetFlow from a single source. If you have multiples, consider using a NetFlow aggregator. You will also need to direct the NetFlow results to your Asset Manager Command Center. These topics are out-of-scope for Asset Manager documentation, but your Solutions Architect and Support can nevertheless help with implementation.

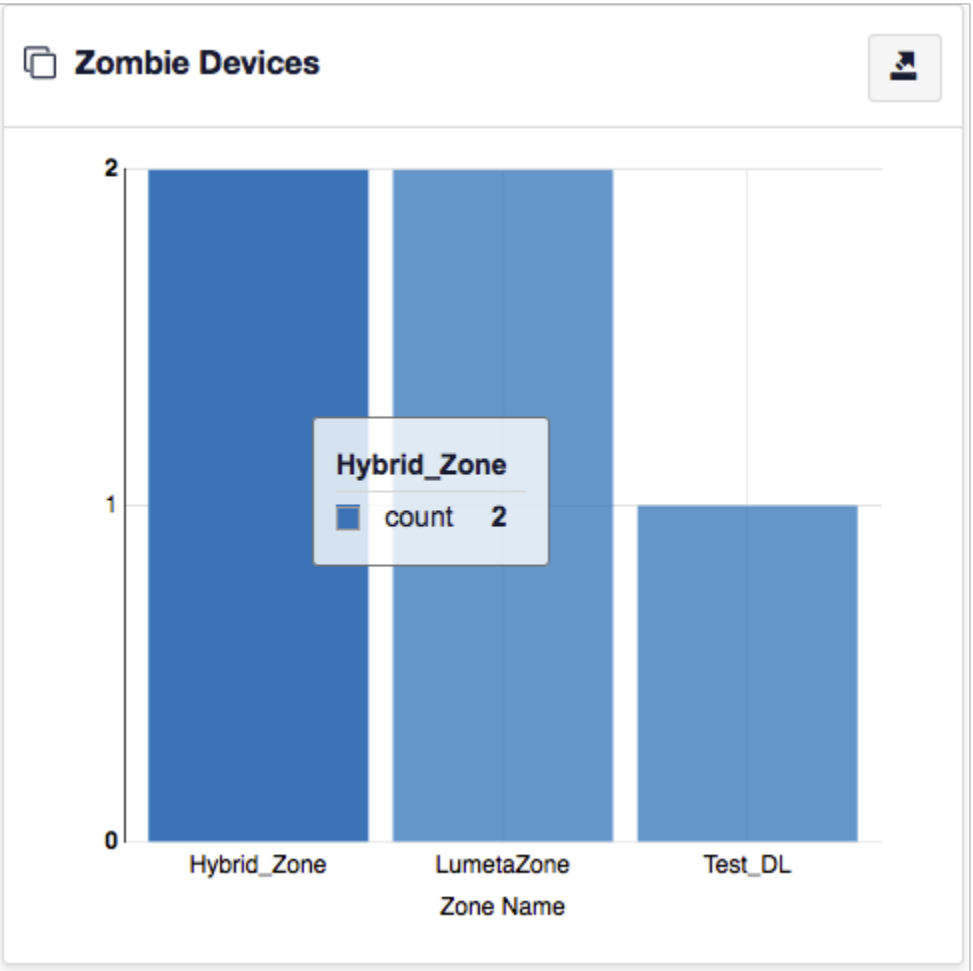


Threat Flows

Destination IP	Source IP	IP in threat	Threat Attribute	Source Port	Destination Port	Protocol	zonename
65.246.245.11	93.174.93.181	93.174.93.181		50783	22	TCP	Hybrid_Zone
65.246.244.14	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.246.100	93.174.93.181	93.174.93.181		50783	22	TCP	Hybrid_Zone
65.246.242.134	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.241.135	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.244.4	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.246.128	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone
65.246.244.87	93.174.93.181	93.174.93.181		50783	22	TCP	LumetaZone

Records 1 — 20 of 380 Page 1

You do not need NetFlow data to show the zombie devices in your network. This dashboard is generated using native Asset Manager-indexed data.



The iDefense feed is correlated against NetFlow data. The intersection of the two populates the threat_feed_ip table. Navigate to **Settings** > **Tables** > **threat_feed_ip** > **View** to open the table.

To configure the feed . . .

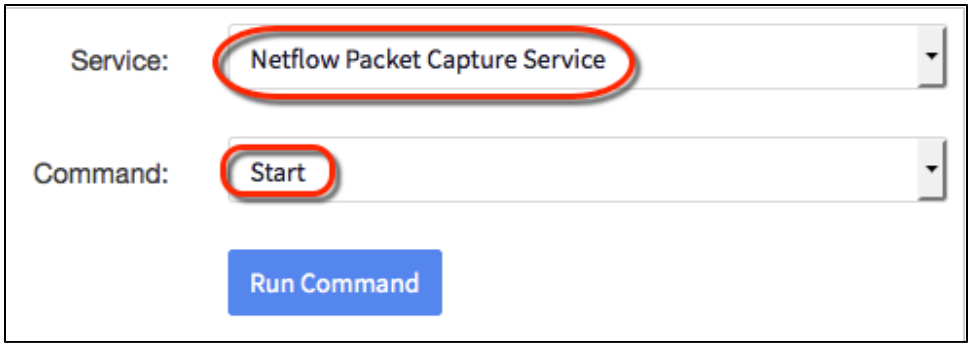
1. Enable the capture of NetFlow data.
2. Configure and enable iDefense in Asset Manager.

Enable NetFlow

The NetFlow-capture service enables your Asset Manager Command Center to ingest NetFlow data.

To enable NetFlow capture from the Asset Manager GUI:

1. On the Asset Manager toolbar, navigate to **Settings** > **Support Tools** > **Status of Asset Manager Components.**
2. Start the Netflow Packet Capture Service and click **Run**.



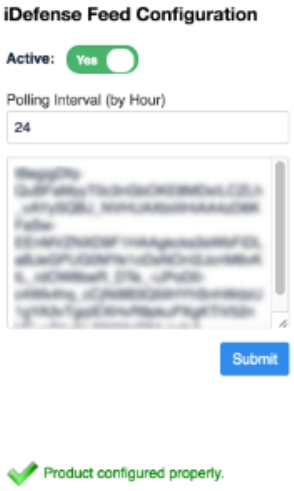
The status of the service will change to Running.

To enable NetFlow capture from the Asset Manager command-line interface:

1. Log in to the CLI.
2. At the command-line prompt, enter **`support service packetcapture start.`**
3. Exit the CLI.

Configure the iDefense feed as follows:

1. On the Asset Manager toolbar, navigate to **Settings** > **Integrations** > **iDefense**.



2. Enable the threat feed by switching the toggle to active.
3. Input a Polling Interval to indicate the time that should elapse between fetching the latest feed data. Input 24 to poll daily, input 12 to poll twice a day, and so on.
4. Input an license key from iDefense.
5. Click **Submit**.