Integrating Scrutinizer with EndaceProbe Network History

Plixer

Scrutinizer can be integrated with EndaceProbes to provide a seamless connection to the recorded Network History residing on the EndaceProbes in your network.

This integration enables analysts to pivot directly from an alert in the Scrutinizer console to view the packet history related to that event in EndaceVision.

Connecting Scrutinizer to the network history on EndaceProbes is done by adding a parameterized URL string to the Scrutinizer configuration file.

This parameterized URL uses the Pivot-to-Vision API function to define a pre-configured Investigation in EndaceVision which retrieves the packet history related to a specific Scrutinizer event and displays the results in EndaceVision.

EndaceVision provides a number of traffic visualization tools that analysts can use to filter the packet history, zoom the timeframe in or out and identify specific packets of interest to analyze in EndacePackets or download in a packet capture file for analysis in Wireshark.

The URL parameters specify:

- Which EndaceProbe or InvestigationManager to access to run the Investigation.
- Which Rotation File(s) to search (Rotation Files are where recorded Network History is stored on EndaceProbes).
- The start and end times for the investigation period (these are provided automatically by Scrutinizer in order to select just the packet history relating to the alerted event).
- Which default EndaceVision visualization tools to use in the Investigation.

Editing the Scrutinizer config file

Configuring Scrutinizer to connect to your EndaceProbes is done by editing the Scrutinizer config file.

To edit the config file:

1. SSH into the Scrutinizer Server

2. Edit /home/plixer/scrutinizer/files/applications.cfg

Configuring server and Data Source options

The configuration settings for integrating Scrutinizer with the Network History on EndaceProbes are specified by adding a URL string to the config file using the following URL encoded format:

```
[INTEGRATION NAME], https://[HOSTNAME or IP]/vision2/pivotintovision/?datasources=tag%3Arotation-file&title=Scrutinizer-Investigation&start=%zs&end=%ze&tools=conversations_by_ipaddress%2Cbandwidth%2CtopTalkers_by_ipaddress%2CtrafficOverTime_by_prot&ip=%i, Endace Vision 2 - Investigations
```

Where:

[INTEGRATION NAME] is the name that is used in Scrutinizer's popup menu to identify the integration. It shows up under "Other" in the Reports menu in Scrutinizer relating to an alert. NOTE: It is possible to define more than one URL entry in the configuration file if you wish to. In this case, it's advisable to choose Integration Names that uniquely identify each configuration setting.

[HOSTNAME or IP] specifies the server that you want to connect Scrutinizer to. This will either be the IP address or hostname of an EndaceProbe, or alternatively the IP address or hostname of an InvestigationManager if you want to connect to multiple EndaceProbes simultaneously.

tag%3Arotation-file specifies that all of the active Rotation Files on the EndaceProbe are searched for matching packets. If the URL target is an InvestigationManager, then this specifies that all active Rotation Files on ALL EndaceProbes connected to the InvestigationManager are to be searched for matching packets.

Below is a sample URL that is configured to connect to an EndaceProbe and accesss the data residing in a Rotation File on the EndaceProbe:

Example URL configuration

```
Pivot-to-Vision, https://end_im/vision2/pivotintovision/?datasou
rces=tag%3Arotation-file&title=Scrutinizer-Investigation&start=%z
s&end=%ze&tools=conversations_by_ipaddress%2Cbandwidth%2CtopTalke
rs_by_ipaddress%2CtrafficOverTime_by_prot&ip=%i, Endace Vision 2 -
Investigations
```

EndaceVision has a number of different visualization tools that may be specified in the URL configuration. For more information on what visualization tools are available, refer to the EndaceVision v2 User Guide.

Note: <start> and <end> variables in the URL configuration are ‘zs’ and ‘ze’.To set the exact time for the Rotation File, the time zone settings need to be set correctly on both Scrutinizer, and the EndaceProbe.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com