Closed-Loop Automation

Automation is a key area of focus for all network operators as they strive to reduce operational overhead costs, improve service levels and expand their value-added service portfolios. Closed-loop automation uses feedback derived directly from the network to drive better automated resolution of network events.

Challenge

One area of future focus that has come through strongly from a number of network operators is the desire to automatically manage shifts in network traffic that would otherwise cause a service impact e.g. congestion etc. Many network operators use automated systems (Path Computation Engines, PCE) to map traffic onto their underlying network capacity in an optimized way.

Risk

These systems gather information on network utilization in a variety of ways, but in most cases their view of the network load is focused at the bandwidth level per interface. They do not have more granular visibility of traffic source and destination based on correlation with routing data.

Solution

Arbor Sightline With Insight can provide customers with a highly granular, multi-faceted view into the traffic running across their networks. This visibility can help customers truly understand the traffic on their networks, the services utilized by their customers and how traffic enters and leaves their environment. Sightline With Insight also incorporates Smart Alerts which allow alert conditions to be built around the results of multi-facet queries. These alerts can be propagated via web-hooks, allowing integration with PCE systems. It's more granular visibility of traffic and services, and how they map onto infrastructure and routing topology, can be used to drive better automated decision making within PCE systems when traffic loads change. This integration is being evaluated by a number of customers at present.

Another area of interest is around better automation of DDoS attack mitigation. Arbor Sightline With Sentinel already automates DDoS attack response. Smart Data integration brings additional, unique capabilities allowing a new level of closed-loop automation. Collecting Smart Data for a specific service will give us application-layer visibility and allow the detection of a broader range of attacks. It will also give us an appreciation of a service user's experience of a service, i.e. its performance from the user perspective. This information can be collected during peacetime and then used during an attack to ensure that a mitigation is returning service performance to a normal level from a user perspective.

Summary

This is a massive leap forward as most reporting and automation today is focused around passed / dropped traffic levels, which do not always accurately reflect how effective a mitigation is being from the end user perspective. Additional capabilities are currently being researched by the Sentinel development team.

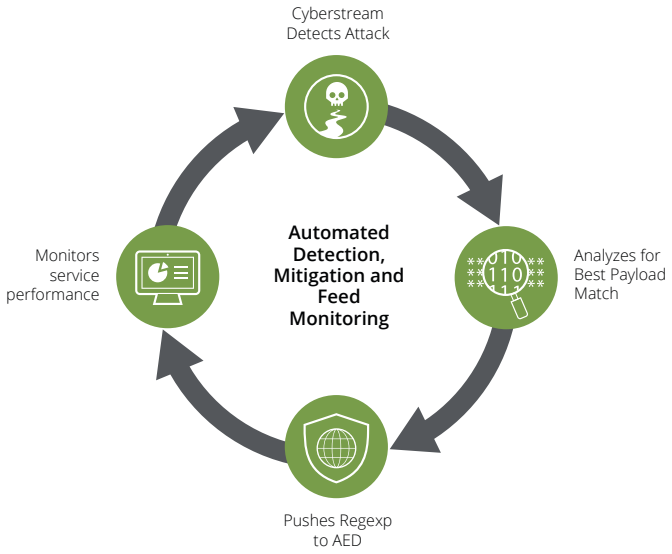

Figure 1: Smart Protection, for Application Threats.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECUC_008_EN-2002 05/2020