Traffic Optimization with NETSCOUT CyberOptimizer

Network traffic growth is one of the biggest data center challenges faced by enterprises and service providers. In today's world, enterprises are challenged with increased threats to their networks and seemingly endless tools to solve security problems. This results in increased network complexity, higher costs and slower response times.

NETSCOUT CyberOptimizer

NETSCOUT® CyberOptimizer is a smart-data-driven software application that improves total cost of ownership (TCO) for packet-based security systems. CyberOptimizer conditions and refines traffic flows before they reach security systems, reducing processing requirements and associated licensing fees. The benefits include:

- **TCO reduction:** Security monitoring appliances look at session and application layer data for patterns to detect security threats, and scaling these to meet the explosive growth in traffic and applications continues to stress budgets and technical limitations. NETSCOUT CyberOptimizer conditions packet flows, reducing noise and the number of new systems needed for future expansion.
- **Reduced risk:** Unlike traditional approaches based on network packet brokers, CyberOptimizer allows users to retain packets for analysis should further forensic investigation be required.
- **Powerful software-first architecture:** Built on the foundation of Adaptive Service Intelligence™ (ASI), CyberOptimizer takes advantage of NETSCOUT's unique capabilities such as Smart Application Filtering to optimize only the relevant traffic and Adaptive Session Trace technology to reduce storage requirements.

Packet Optimization and Filtering

Each deployment and each network have different needs, and typically administrators require one or more features, working together, to provide and deliver the service they need. Below is an overview of some of CyberOptimizer's capabilities.

Smart Application Filtering

NETSCOUT deployments already benefit from the powerful way in which our patented ASI technology allows administrators to not just understand what is going on in their networks in L2 or L3 terms, but rather, in a more natural, application-based way. Extending our ASI functionality to filters is what allows NETSCOUT CyberOptimizer with Smart Application Filtering (SAF) to effectively and easily filter traffic based on application type. Simply identify and then filter on one or more applications, and forward the results on to security tools.

High-performance Packet Archive

When troubleshooting a filter, determining whether a filter appropriately filtered (or not) the correct traffic is often a daunting task. CyberOptimizer enables administrators to save all, or a subset of original traffic, for later recall and replay; no packets are lost due to filtering. Further, just as SAF allows administrators to define filters based on application, packet archive works the same way, allowing administrators to leverage NETSCOUT's Adaptive Session Trace (AST) technology to save a copy of all traffic, or traffic by application(s) type, for later export for replay.

Packet Export and Drilldown

CyberOptimizer provides rich, contextual search capabilities within the archived traffic: by date and time, IP, and applications. It provides packet retrieval, export in packets (PCAP) and NetFlow with enrichments. Take advantage of packet drill downs with decoder for inspection of packets, connections and sessions before export.

Encrypted Traffic Identification and Filtering

Today's networks carry high volumes of HTTPS and encrypted traffic, often more than any other type of traffic. The encrypted traffic using well known ports such as the HTTPS and SSH traffic could be easily filtered and removed, but this complete removal poses a potential security vulnerability. Many of the security tools are specialized and requires only a subset of the network traffic for their investigation. Some application traffic today doesn't use industry-standard ports, while intruders often change the ports making illegitimate traffic harder to track. Optimizer uses heuristics to detect these ports and filter out the encrypted traffic.

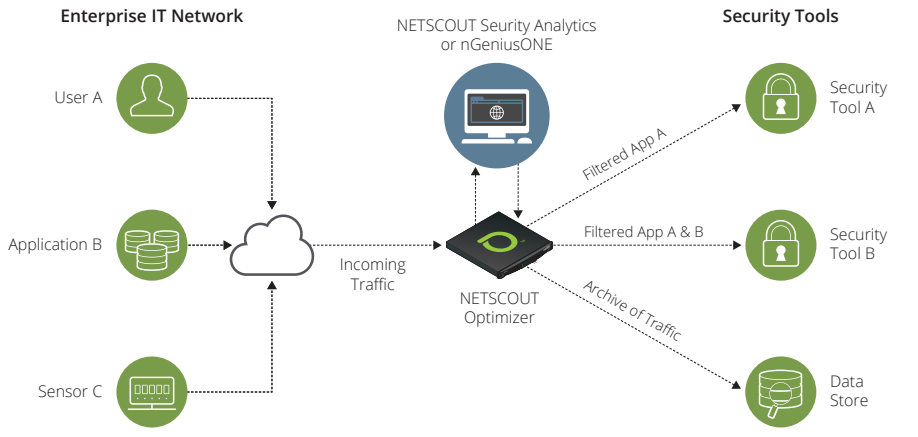

Figure 1: Traffic optimization with NETSCOUT CyberOptimizer.

NetFlow Generation

Where needed, CyberOptimizer generates NetFlow (versions v5, v9, and IPFIX) and export to up to four NetFlow destination collectors, and detailed flow statistics available.

Protocol Header Stripping

Some security tools don't care or won't function with certain packet headers intact, and prefer to see only, for example, the payload of the packet. CyberOptimizer performs header stripping, with the ability to remove VLAN tags (one, two, or all VLAN tags), MPLS headers (up to seven labels), GRE, NVGRE, and ERSPAN headers, and GTP headers.

Deduplication

Deduplication functionality allows CyberOptimizer to remove multiple copies of the same packet from the traffic stream, such that the destination security tool receives only one copy of the packet.

Packet Slicing and Masking

Depending on the network and environment, some deployments require a "complete" packet to be sent to the security tool, but for a variety of reasons (internal policy, legal compliance, etc.) information within the packet is deemed sensitive and must be changed, or masked. CyberOptimizer performs this masking function, allowing for complete traffic streams to be sent to tools while masking, or covering, sensitive information within the payload.

Packet slicing, unlike masking, removes part of the packet altogether before sending it on to its destination. CyberOptimizer performs packet slicing based on a variety of configurable options (ETYPE, IP protocol).

Configuration

CyberOptimizer is configured and managed by NETSCOUT's nGeniusOne® interface. With a powerful but easy to use web browser-based user interface, nGeniusOne allows administrators to configure, monitor, and troubleshoot all of CyberOptimizer's features from a single pane of management. CyberOptimizer is also available for configuration via NETSCOUT Security Analytics, enabling administrators to manage their security solutions from a common pane of management.

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

PFSQL_010_EN-1801 10/2018