Tool Chaining

BUILDING A TOOL CHAIN

How to be sure that everyone gets the right thing when everyone wants everything

The Challenge

Ensuring that the network is running at optimal speed is a business imperative. Zero downtime — or close to it — has become a competitive differentiator. In such an environment, security and privacy are not only absolute requirements but essential to the well-being of the business. In order to meet these sometimes competing objectives, networking professionals must have complete visibility into every element of the network, at all times. They must also be able to look into the future, to see and mitigate possible issues before they occur.

Meeting today's business requirements on the network presents several challenges, particularly when you consider the number of different analyses, performance and security tools that may need access to the same data stream. Furthermore, in many cases each toolset is managed by different individuals or groups. Each group has its own requirements and concern and its own dedicated tools designed to deliver the information it is mandated to provide. To complicate matters further, each tool may need a slightly different form or portion of the same traffic; in the case of servers, for example, one group might want to see web threads, while another group needs to see overall web application performance. Complex rules and specific network designs must be created to ensure that traffic flows are properly articulated and understood for each tool.

The Solution

NETSCOUT Packet Flow Switching

In this climate of competing goals, an increasingly complex threat environment and complicated reporting requirements, the NETSCOUT packet flow switching technology offers a solution that is both simple and elegant and provides every stakeholder with all the information they need to achieve their objectives; in other words, this solution is able to give everyone what they want. NETSCOUT makes it possible through its nGenius packet flow switches that enable an organization to deploy a comprehensive inline security infrastructure in a virtual chain, rather than each tool being its own actual physical bump in the wire. Each tool can still get exactly the traffic it requires, at the speed and in the form that it is designed to accommodate.

Each nGenius packet flow switch provides the assurance of network uptime and continuous monitoring that is required.

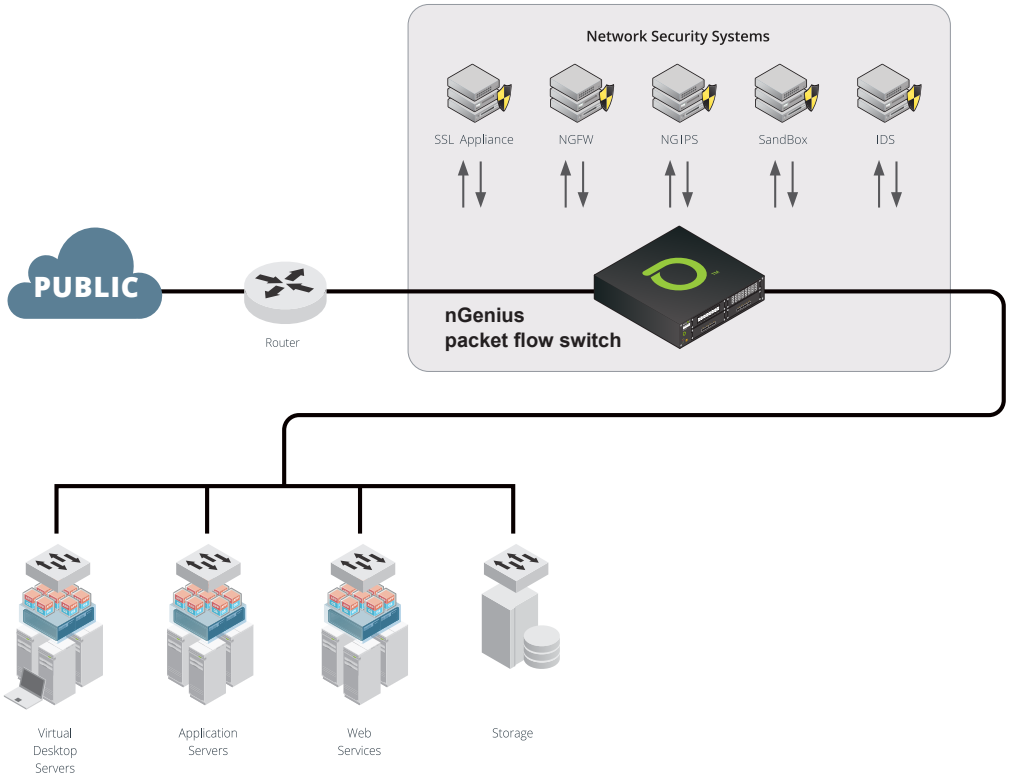
As an example, these tools may include security systems such as NGFWs, IDS, IPS or sandbox solutions. Traffic is then examined by each security device and once the inspection is finished, the traffic is sent back to the packet flow switch, which forwards the traffic to its final destination. This "aggregate once, serve many" approach enables every tool to get the type and portion of the traffic they need. At the same time, from the network's perspective, there is only a single appliance — the packet flow switch — on the wire.

Value

There are many benefits to deploying an inline tool chaining solution. One of the most visible benefits is the decoupling the security devices from the network. The convenience of the NETSCOUT approach can be crystalized in the ability to:

- Make changes to the security devices (software and hardware upgrades, adding more devices, removing old devices, etc.) without requiring network outage or maintenance window.
- Change the security devices' configuration and/or the order in which they are used without any physical changes or impact to network traffic.
- Exclude malfunctioning tools without affecting the network in any shape or form.

With NETSCOUT, network security, performance, and monitoring tools can use packet flow switches to actually transcend their physical location. That's because, regardless of the physical location of the packet flow switch, they are all interconnected logically, as are the tools to which they are attached. This fact delivers peace of mind for security ops while at the same time minimizing conflict between networking and security teams. With NETSCOUT, everyone gets what they want.



Providing visibility to a set of 5 security devices provides an excellent example of the NETSCOUT functionality.

In this scenario:

- Traffic comes into the packet flow switch which starts filtering traffic according to the policies created by the operator.
- In this case, the packet flow switch forwards the encrypted traffic to an SSL Visibility appliance designed to decrypt the traffic and the non SSL traffic is sent to the next device in the toolchain, a Next Generation Firewall.
- The traffic unencrypted by the SSL decryptor is then sent to the Next Generation Firewall

The packet flow switch can then forward the appropriate portions of the now decrypted traffic to the other tools (both active and passive) that need to examine it.

This joint solution delivers:

- End-to-end visibility for threat identification, investigation, and resolution
- Security service chaining to achieve a combined active and passive security posture
- More time spent in research and resolution and less time administering security infrastructure

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000