NETSCOUT and Blue Coat: Visibility into SSL Traffic

Advanced persistent threats and attacks continue to target and infiltrate organizations on a daily basis forcing these enterprises to continually enhance their security postures and capabilities. To keep pace with the changing threat landscape, organizations not only need to adopt proactive approaches and enable continuous improvement in security deployments, but also reduce risks and minimize the impact of changes on network operations and costs. Threats are becoming more sophisticated and targeted, including attacks hidden in previously trusted technologies like SSL encryption.

In fact, industry analysts have predicted that by 2017 around 50% of all network attacks will be inside SSL tunnels; furthermore, the amount of enterprise SSL traffic will continue to increase at a rate of 20%. This significant amount of traffic is, clearly, a very attractive target for bad actors. Security tools such as Next-Generation Firewalls (NGFWs), Intrusion Detection/Prevention Systems (IDS/IPS), Data Loss Prevention (DLP), analytics and malware may be blind to the growing amount of traffic that is being encrypted within SSL, creating security challenges. Getting and staying ahead starts with a pervasive and proactive defense architecture employing multiple security systems and requires access to all the traffic flowing through the network. It also demands an approach that reduces risks and impact on network operations and costs.

NETSCOUT nGenius Packet Flow Switches and Blue Coat SSL Visibility Appliance

NETSCOUT enables a proactive approach to security visibility that helps organizations accelerate advances in cyber security posture, capabilities and responses. An essential part of this process is providing visibility into traffic encrypted by SSL. The Blue Coat® SSL Visibility Appliance is a high-performance, purpose-built solution that utilizes comprehensive policy enforcement to inspect, decrypt and manage SSL traffic in real time while ensuring data privacy and regulatory compliance.

Comprised of the NETSCOUT nGenius® packet flow switches (PFS) and Blue Coat SSL Visibility Appliance, the solution enables security teams to adopt a "decrypt once, feed many" design, empowering multiple security systems. By providing visibility into previously hidden traffic, advanced threats can be revealed without requiring significant upgrades or re-architecting the network security infrastructure.

The combined solution decrypts traffic so that it can be forwarded to multiple passive, active inline and large-scale advanced threat defense security systems allowing them to concentrate in performing their assigned functions. Network visibility into the encrypted traffic effectively detects and eliminates advanced threats without hindering device or network performance.

The SSL Visibility Appliance gives the nGenius packet flow switches visibility into all SSL traffic and applications to close the security visibility loophole created by encrypted traffic. In addition, it has the ability to selectively decrypt and inspect suspicious or unknown encrypted traffic while not inspecting other SSL traffic due to mandates such as HIPAA, SOX, PCI, Sarbanes-Oxley, etc.

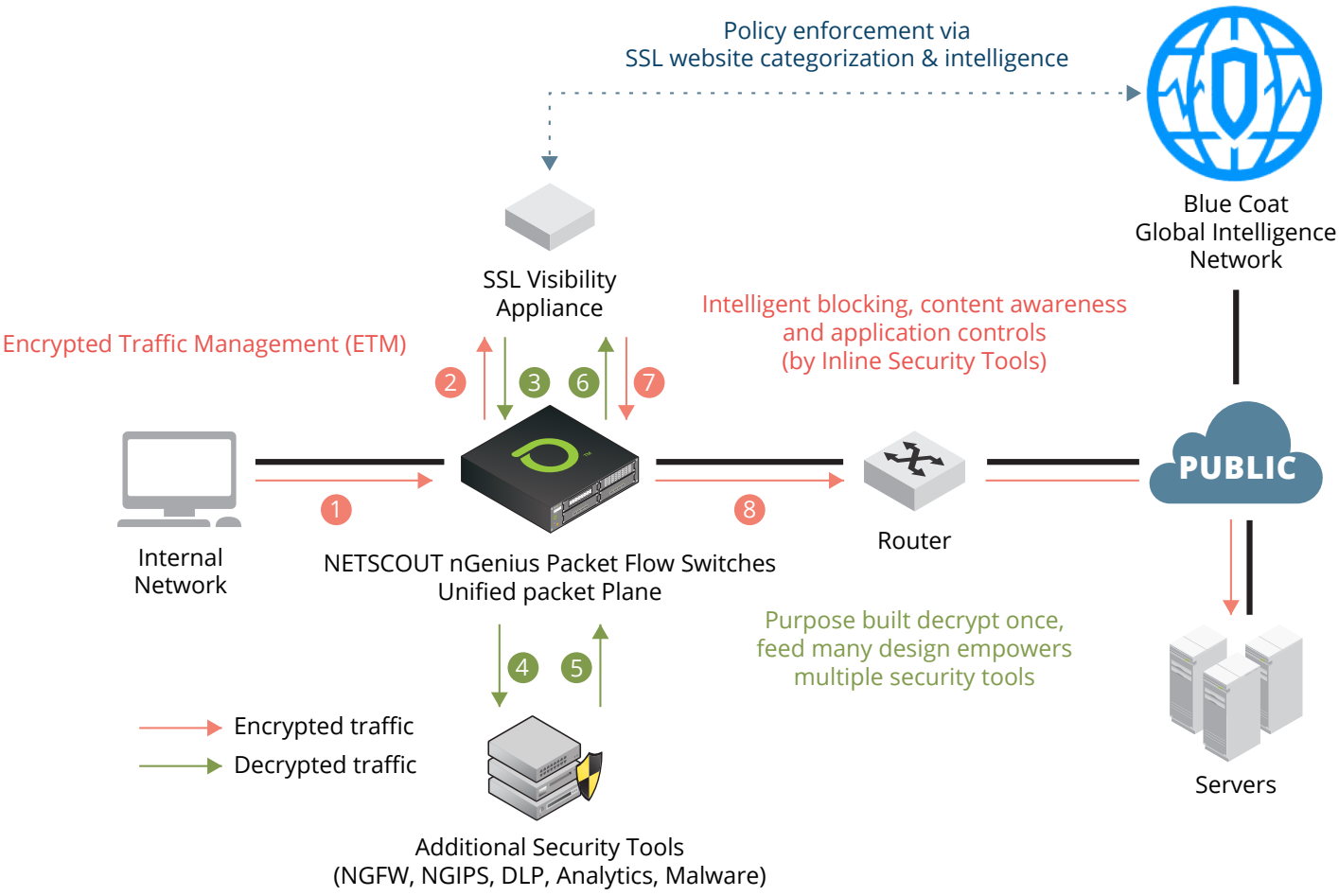
In today's security deployments, multiple security systems need to be combined, served and service-chained. NETSCOUT leverages years of experience building security visibility capabilities for global customers. This joint solution combines the capabilities of the SSL Visibility Appliance to inspect and decrypt SSL traffic with the NETSCOUT unified packet plane, sending relevant decrypted traffic to any or all of your security tools as needed.

Solution Design

The diagram below demonstrates how the combined Blue Coat and NETSCOUT solution work to provide best-in-class encrypted traffic management. This example shows a design using the Blue Coat SSL Visibility Appliance with the nGenius packet flow switch, which provides a dynamic, flexible, and cost-effective solution for any network. The joint solution provides visibility and data access across the network for centralized or distributed security tools, and supports flexible designs for both passive and active inline security tools.

How it Works

1. nGenius 4200 series packet flow switch (PFS 4204) receives traffic from the internal network.
2. PFS 4204 passes only SSL and Port 443 traffic to the Blue Coat SSL Visibility Appliance. This allows the Blue Coat SSL Visibility Appliance to perform decryption at a very high rate.
3. The Blue Coat SSL Visibility Appliance makes a copy of and decrypts the copied traffic, and then sends the decrypted traffic to PFS 4204.
4. PFS 4204 sends the decrypted traffic to any or all of the additional security tools that are required to have visibility into the data, either sequentially or in parallel, based on either their passive or active nature. These tools then decide whether the decrypted SSL traffic should be allowed to continue to the desired external servers.
5. The security tools return their results to the vBroker.
6. PFS 4204 returns the traffic to the Blue Coat SSL Visibility Appliance.
7. The Blue Coat SSL Visibility Appliance determines whether the original encrypted session should continue or be reset. If it determines it can continue, the encrypted SSL traffic is returned to PFS 4204.
8. If the traffic is permitted, PFS 4204 sends the encrypted SSL traffic to the desired external servers, where policy enforcement, categorization, and intelligence are provided by the Blue Coat Global Intelligence Network.



About NETSCOUT nGenius Packet Flow Switches

NETSCOUT nGenius packet flow switches optimize the flow of traffic from the network to the security systems and monitoring tools. These appliances collect and organize packet flows—creating a unified packet plane that logically separates the network layer from the tool layer. Our customers use packet flow switches to optimize and scale both their service assurance platform and cybersecurity deployments so that they can spend less time adding, testing and managing their tools.

About Blue Coat

Blue Coat is a leader in advanced enterprise security, protecting 15,000 organizations every day, including 88 of the 100 largest global companies. Through the Blue Coat Security Platform, Blue Coat unites network, security and cloud, providing customers with maximum protection against advanced threats, while minimizing impact on network performance and enabling cloud applications and services. For additional information, please visit http://www.bluecoat.com.

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