NETSCOUT

Unlock Optimized Active Security

4 Key Questions You Need to Ask

The threat landscape is evolving, and so are the security systems designed to address it. But this resulting tool sprawl places new demands on operations. Every change or upgrade means a potential network disruption.

A packet flow switch (also known as a network packet broker) is the optimal solution to the challenges that come with scaling your monitoring infrastructure to keep up with the demands of modern cybersecurity. But how do you identify the solution that's right for you?

Here are the four key questions you need to answer when evaluating a packet flow switch to support your active security deployments.

NETSCOUT

How does the solution identify and track packets?

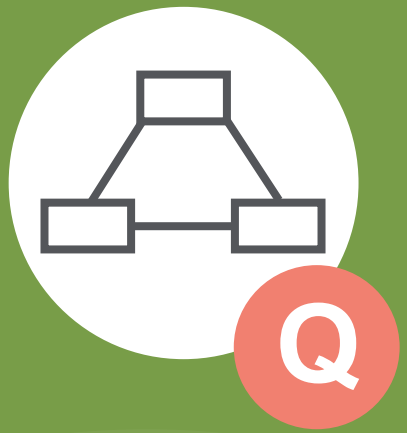
When aggregating active security traffic, knowing where packets are coming from is vital for ensuring return delivery to the correct network segment. Often, this is managed using additional VLAN tags, but many active security tools can't handle excessive VLAN tags. This leads to dropped packets, skipped inspections, and blocked traffic that exposes your enterprise to security risks and network disruption.

Look for a solution with active inline aggregation translation.

A packet visibility appliance capable of supporting today's critical security solutions needs to be able to track packets at line rate without appending extra VLAN tags.

NETSCOUT

2



How much network protection and redundancy does the solution provide?

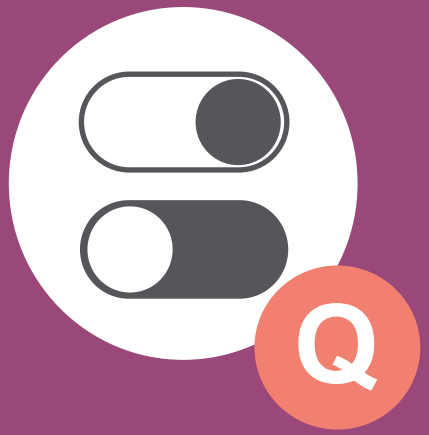
Typical solutions require both a primary (active) and secondary (stand-by) visibility appliance to handle redundancy in the event of power failure. This approach is difficult to scale. In addition, it results in a dedicated stand-by device that is otherwise not contributing to the task of processing and forwarding traffic.

Optimize your resources with a solution that provides efficient redundancy.

Prioritize an efficient packet visibility solution that can optimize packet flows and provide availability by enabling the use of secondary appliances, that would normally be idle, for directing traffic to other security systems using customizable trigger policies.

NETSCOUT

3



How does the solution ensure that security systems are functioning optimally?

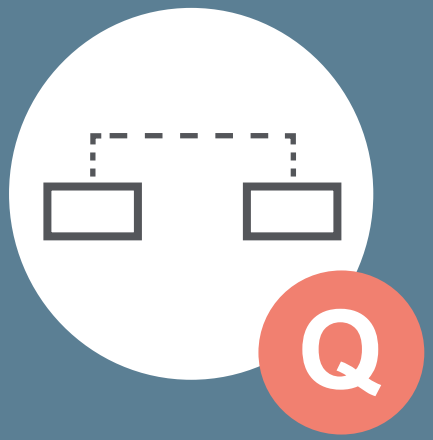
While most solutions support positive health checks, be warned: this only provides a simple on/off response that fails to show if security appliances are performing as expected or if they may be in a “bypass” mode and letting uninspected traffic through.

Make sure your solution can perform negative health checks supported by flexible trigger policies.

Negative health checks verify whether security systems are doing their jobs and stopping malicious packets. For improved efficiency, look for a solution that can respond to health checks by automatically redirecting traffic to other security systems while alerting the security team that a system needs attention.

NETSCOUT

4

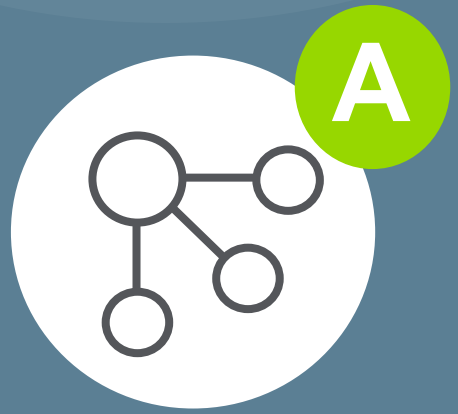


What load balancing options are possible with the solution?

With many enterprises moving to the cloud and an increasing variety of data sources and destinations, agile and flexible load balancing is essential when distributing traffic to multiple instances of the same security systems.

Go with a solution that supports session-aware load balancing.

Choose an approach that can accommodate a wide variety of hash options. This is necessary for improving visibility into packet flows when their source or destination data may obfuscate information that is important for efficient and secure load balancing.



NETSCOUT

For packet visibility in active security deployments, you cannot afford an underperforming system that lacks flexibility and has limited functionality. Packet flow switches can help any network scale to keep up with today's modern threat landscape.

Looking for a packet visibility solution that can optimize your present and future security systems? Choose wisely. Opt for one with the features that matter.

Learn about the nGenius™ packet flow switch here:

www.netscout.com/solutions/enterprise/security-visibility