IP Tunnel Termination in the Packet Flow Switching Layer

IP Tunnel termination capability allows copied traffic to be forwarded, as a remote SPAN function, over an IP network from a virtualized environment to a nGenius® packet flow switch for the purpose of service assurance or security monitoring, for any network link speed.

Background
Monitoring virtualized “east-west” traffic between virtual applications, where the traffic never leaves its virtual server environment (VSE), requires a way to access and forward the traffic from within a VSE out to a packet flow switch for distribution to the various monitoring applications employed for service assurance and security purposes.

There are several methods for accomplishing this, where the most common is using a remote switch port analyzer (SPAN) function to encapsulate and forward the traffic out over an IP network link. This can be referred to as unidirectional IP tunneling.

Terminating the IP Tunnels
When traffic is tunneled out from a VSE, it needs to have a destination. The logical and best place for the destination is a packet flow switch port connected to the IP network.

Other network packet broker (NPB) solutions for addressing this tend to be monolithic, rigid, and expensive. These solutions almost always require the use of dedicated hardware, have performance bottlenecks, are restricted to only a couple of encapsulation types, and always remove the encapsulation which could be useful for the monitoring applications.

NETSCOUT Solution
The NETSCOUT solutions for IP tunnel termination offer a number of options to match their architectural and network monitoring needs. This includes the ability to choose a custom-hardware or disaggregated solution, choose an appropriate solution for throughputs from 10Gbps up to 4Tbps, handle almost any type of unidirectional IP tunneling protocol, and decide whether to de-encapsulated the tunneled traffic or not prior to forwarding to the monitoring applications.

nGenius PFS Capabilities
The various capabilities for IP tunnel termination across the nGenius Packet Flow Switch (PFS) family include protocol support, throughput performance, and architectural.

Protocols
NETSCOUT supports any tunneling protocol, as long as it uses IP as the transport layer, is unidirectional, and does not require any handshake or response. Typical protocols used include GRE, L2GRE/NVGRE, and ERSPAN.

• Termination of the tunneling protocols is supported today on the nGenius 2200, 4200, 5000, and 6000 series packet flow switches and on the nGenius Packet Flow eXtender (PFX) software.
• De-encapsulation of the traffic from the tunneling protocols is supported on nGenius 2200, 4200, and 6000 series packet flow switches with an advanced module, nGenius 6000 series packet flow switch with an advanced module or card, and PFX. Please refer to the "Protocol Stripping/De-encapsulation Using NETSCOUT nGenius Packet Flow Switches" paper for more details.

Throughput
The maximum throughput of terminating the tunneled traffic that is supported by the products mentioned above is effectively the same as the total throughput of each of the products. There are some performance limitations regarding responding to ARP and ICMP (“ping”) messages, but for most realistic network situations, there would not be any performance limitations.

Architecture
There are two approaches that users can select from for their monitoring fabric infrastructure, being the more traditional integrated software and hardware versus the disaggregated hardware and software options.
The advantage of the nGenius PFS solutions are that the tunnel termination can be performed by any of the products, regardless of the architecture. It is only if and when a user needs to de-encapsulate the monitored traffic from the tunnels, for one or more monitoring applications, that the decision of which architecture to adopt may become important. Figure 2 to Figure 4 show examples of the two architectural approaches using the nGenius PFS family.

**Custom Integrated**

nGenius 2200, 4200, PFS 6000 series packet flow switches offer a fully integrated, custom hardware architecture where the IP tunnel is terminated on any port, and de-encapsulation for the tunneling protocols is conducted in the integrated advanced hardware.

**Disaggregated**

PFX is the key in a disaggregated approach to performing the IP tunnel termination and tunnel de-encapsulation. In the case of the nGenius 5000 series packet flow switches, the PFX is only required for tunnel de-encapsulation. In the case of nGenius 3900 series packet flow switch, PFX is required for the IP tunnel termination as well.

---

**Figure 2: Custom Integrated Hardware and Software.**

**Figure 3: Disaggregated Hardware and Software with nGenius 5000 series packet Flow switch and PFX.**

**Figure 4: Disaggregated Hardware and Software with nGenius 3900 series packet flow switch and PFX.**