

Monitoring: TAP vs SPAN

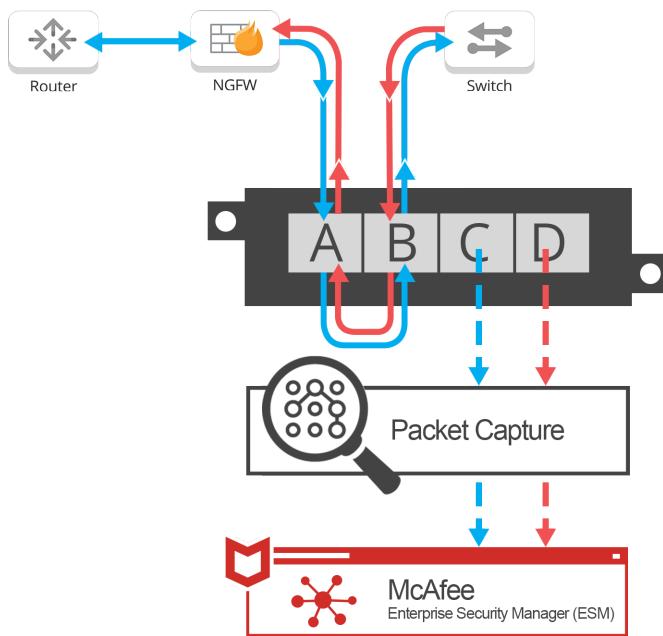
When Packet Capture is Mission Critical

The US Army regularly participates in the DoD's Warfighter, an information technology exercise testing the command center's ability to do mission command and mission control tactical communications between units in the field.

During setup for a recent exercise, the team ran into immediate issues with their sniffers due to packet loss. This can be attributed to using the switches' SPAN ports (Mirror Ports) as the access method for the sniffer. The packet loss was due to configuration issues, which lead to the port being rendered permanently inoperable, and even caused the entire division's headquarters building to go down.

Painpoints:

- Packet loss through the reliance on SPAN was our biggest problem, causing network downtime.
- Essentially our cyber network defender analysts would not be able to do their job, at least within the wire, to make sure that nefarious activity isn't going on within the network.



Solution: These issues justified the need for network TAPs. "We did a little bit of research and found that network TAPs were definitely the superior option when it comes to capturing network traffic." -Sergeant, Cyber Ops Specialist (17C), 82nd Airborne Division

Garland Technology's XtraTAPs feed wire data to SecurityOnion's sniffing interface to capture the traffic and forward all the logs for the routers, all the switches, anything within the network infrastructure to McAfee Enterprise Security Manager, ESM, which gives alerts if there's anything beyond Palo Alto Networks' NGFW to analyze.

"[Garland] is engineered, designed, made in America. With anything these days, especially with technology, you have to be fairly careful what you buy."

-Cybersecurity Chief,
82nd Airborne Division

Value:

- Provide 100% wire data for packet capture.
- The Garland Quality Standard: All TAPs are stress tested with live network data and validated.
- Made, supported and serviced in the USA.

This document is for informational purposes only. The information in this document, believed by Garland Technology to be accurate as of the date of publication, is subject to change without notice. Garland Technology assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains. Garland Technology's XtraTAPs are not endorsed by the US Army or 82nd Airborne Division. ©2019 Garland Technology LLC. All Rights Reserved