NIAGARA NETWORKS

Case Study

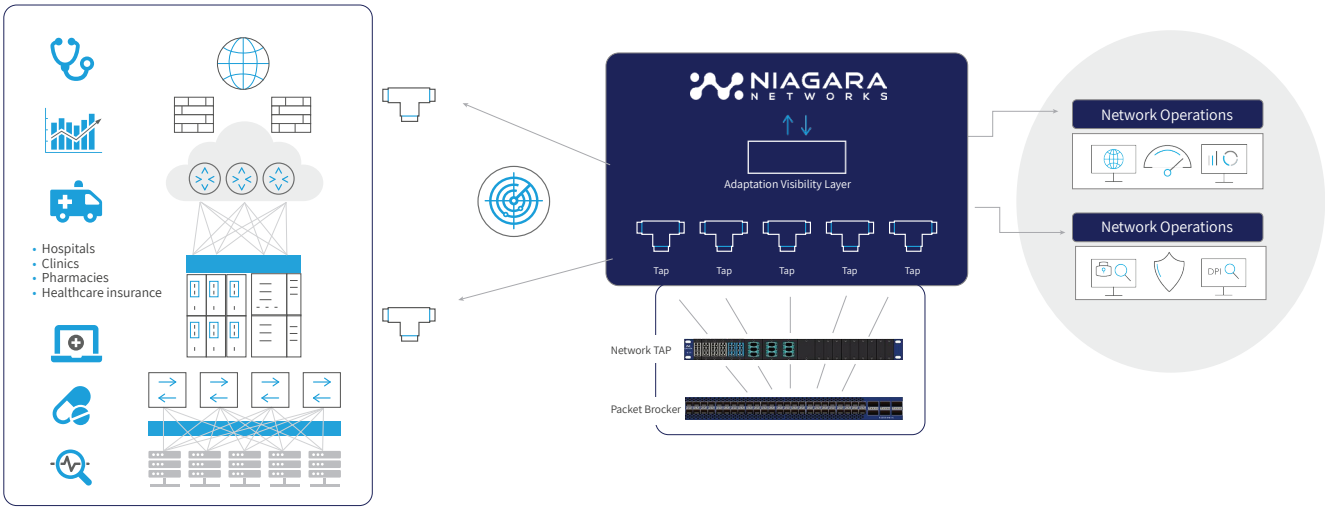
Large Government Healthcare Organization Solves Network Visibility Complexity with Niagara Networks

Agency Gains Flexibility to Quickly and Easily Deploy New or Different Security Solutions as Needed

Challenge

Healthcare sector is at the massive stage of digital transformation. As healthcare operations move to electronic medical records and internet enabled services, they have been mandated to comply with privacy regulations with the best security protocols to protect highly sensitive records of their patients across their IT infrastructure. With new telemedicine and high capacity data (MRI and other digital images) traversing local and remote networks, optimization of traffic, masking of medical data, encryption and complete end-to-end visibility on entire digital processes and assets is paramount. A large managed healthcare organization headquartered in the US faced security and networking challenges as they accelerated their digital transformation. IT operational processes required agile access to traffic as there were no available SPAN ports on existing equipment to allow incremental deployments of security solutions needed for best practices or required by compliance. They faced the common problem of tool sprawl with its parallel challenge, limitations on available ports. While some organizations can, and must, "rip and replace" existing solutions to make way for new ones, many do not have this option.

The organization set a goal of regaining control of SPAN ports from existing devices and the desire to provide a new level of flexibility and simplicity for needed deployments of security and networking solutions. In particular, they needed to increase their monitoring footprint in conjunction with nearly constant network expansion while enabling the adoption of more security analytical tools.



Solution

The healthcare organization turned to Niagara Networks to solve network visibility complexities by implementing a dedicated network TAP solution that enables the greatest ease and flexibility of adding tools or security products to the network or making changes. A network TAP (Terminal Access Point) is an external network device connected to the network that creates a “copy” of the traffic for use by various security solutions monitoring devices. It provides traffic mirroring and is an intricate part of an organization's network stack. The network TAP device can be introduced at any point in the path of the network needing observation, so that it can copy data packets and send them to a monitoring device or tool. Based on optical splitter technology, the appliance always stays connected to tapped network point. It does not need its own power supply and is fully secure and invisible, with full transparency to IP, MAC addresses or any configurations and bandwidth rates.

The organization replaced its existing SPAN port with physical network TAPs from Niagara Networks. The physical TAP platform had more than enough expansion room to replace the SPAN ports as well as provide additional for future growth. In addition, the company can later aggregate the multiple TAP links to accommodate even more needs in the future by grooming all intercepted traffic to Network Packet Broker solution and enable highly efficient aggregation architecture that can be deployed and provisioned by Niagara’s SDN-based software orchestration controller. They can also migrate to the Niagara Networks Open Visibility Platform in the future if they need solutions hosted virtually on a single appliance and have need for traffic processing, such as selective decryption, masking or de-duplication. The Niagara Networks TAP appliances can be selected as passive or active as per designer preferences and offer transparency to network speeds offers high flexibility to intercept traffic at 1Gbps, 10Gbps, 25Gbps, 40Gbps and 100Gbps and traversing communication protocols.

After deployment of the Niagara Networks visibility solution, the organization can deploy and migrate applications in less than five days as opposed to 30 days or not at all. They also saw reduction in DC footprint 4:1 and performance boosts of 25-40%

> “Niagara Networks not only solved our port shortage but opened up new potential for solution flexibility and ease of deployment,” said a Network Architect from the agency. “With Niagara Networks we have been able to modernize our network and be fully prepared to meet the challenges of a constantly changing network and evolving requirements.”

Value Proposition

- Great flexibility to deploy numerous solutions without facing limitations in available SPAN ports
- Effective alternative to SPAN ports - collects 100% of network traffic including error packet that SPANs may drop (a SPAN port deletes corrupt packets and packets below minimum size; also SPAN ports often don’t allow VLAN tags to pass through, making it difficult to detect VLAN issues and creating false issues. TAPs allow all traffic to go through, which prevents these types of issues)
- 100% secure and invisible, no IP address, no Mac address, it cannot be hacked
- Performance boosts of 25-40%
- Plug & play, no configuration, easy installation– fully photonic, no power source required and no IP configurations
- Attractive OPEX and CAPEX with optimized aggregation of TAP elements and operational simplicity
- Ability to intercept 100% of traffic at 1Gbps, 10Gbps, 25Gbps, 40Gbps and 100Gbps and any traversing communication protocols
- Compact form factor – fully modular and flexible - up to 25 TAP links (dual fiber and BiDi)
- Ability to migrate to Niagara Networks Open Visibility Platform for NextGen virtual tools adaption and operational agility