CASESTUDY

STARLINK
TRUSTED SECURITY ADVISOR

StarLink successfully closed a large deal with one of the biggest government clients from UAE.

OVERVIEW

After the client expressed dissatisfaction with their organization's existing firewalls, StarLink was contacted by the information security team to explore alternative "next-generation" firewall solutions. StarLink having evaluated the situation knew exactly what the best solution was.

THE CHALLENGE

In early 2015, the client expressed concerns with their existing firewall solutions. They realized that they needed an upgrade on their current network pipe from 1 Gbps to 10 Gbps fiber at the core switch end. StarLink noticed that their existing firewall was not technically capable of the network upgrade. The client was also using a traditional stateful inspection firewall that controlled traffic based on port addresses. However, the client was apprehensive about the problems that would arise once these requirements were met. For instance, would their firewall performance withstand the heavy traffic as the result of increasing the speed at the core switch? Would its firewall performance be compromised? Other related concerns were, would they able to be monitor the heavy user traffic on the firewall? Would there be a latency in the network due to multiple inspection engines like Antivirus, IPS, Antispyware, firewall, URL filtering due to added load?

THE SOLUTION

As a value added distributor and a trusted security advisor, StarLink analyzed the situation and came up with efficient and effective solutions to help secure the client's network. They advised on using a leading next generation firewall security and IPS as a solution.

Firstly StarLink incorporated SFP+ transceivers that are the most efficient to transmit Ethernet traffic in the network thereby ensuring no problems would arise due to the upgrade of the network pipe.

Next StarLink introduced a solution that identified the application based on its unique properties and characteristics instead of classifying the traffic by port and protocol. Certain applications like VPN also require the firewall to dynamically open pinholes to establish connection and determine the parameters of the session. For such applications, the firewall serves as an Application Level Gateway as it opens a pinhole for a limited time to exclusively transfer data with the ability to enforce policy at the application layer. This was a welcome upgrade from the traditional stateful inspection firewall that the client had in use.

StarLink was well aware that the client's current firewall performance would be affected by the heavy traffic on the network.

Whenever there was a software update or appliance management was done on the existing firewall the whole performance of the network was affected. The suggested solution was to use an efficient application

firewall that segregates management connection and data connection. The traffic processing is segregated where there is a separate management plane for management traffic and a separate one for data traffic which means that there are dedicated hardware components (processor, memory storage etc) inside the appliance solely for management of the appliance which includes software updates, appliance management, dynamic updates etc. This set of hardware is not used for data connection which includes all production traffic that needs to be controlled by the appliance. All firewall inspection, URL filtering, IPS Inspection and Antivirus Inspections are performed in this dedicated control plane which has its own set of hardware components. This segregation thereby increases the performance of the appliance to get optimal performance.

StarLink's solution enabled the client to monitor user traffic on the firewall and view the traffic logs with the exact username that was bound to the traffic.

This further allowed control and policy based visibility over users which efficiently leverages user data in an active directory for logging policy creation and reporting. Lastly, to prevent latency in the network because of multiple inspection engines, StarLink's solution used a single-pass architecture which enforced inspection of the packet from all engines at the same time.

CONCLUSION

To conclude, StarLink induced a technology that is a blend of function specific processing, custom hardware and high end software design to offer excellent visibility, optimal performance and low latency throughput.