Wysetek Implements Next-Gen Firewall for a leading bank

WYSETEK

Palo Alto firewall prevents known and unknown threats and is capable of blocking known threats, including exploits, malware and spyware.

The customer is amongst the top public sector banks in India. The Multi-State Scheduled Urban Co-operative Bank stands among top 10 co-operative banks of the country with many awards under its belt for its contribution in the banking sector.

Business Requirement

The industrialization of hacking and the increase in volume, velocity, variety, and sophistication of threats by today's threat actors is becoming a big problem for all industries including the banking industry.

As the threat landscape is continuously evolving, there is a dire need for banks to protecting the assets – internal and external (their customers). Hence the various security solutions helps cover these requirements and secure their infrastructure from foreign invaders or possible breaches.

The multi-state co-operative bank wanted to strengthen their security posture across its branches across Indian cities and states. They were looking for a solution that prevents both known and unknown threats across its main office and the distributed offices across India. With mobile banking and Apps being the norm of the day, they wanted a security solution that also protects their Apps and its users.

The Solution

Wysetek team studies business requirements of the customer and its operations. Wysetek team extensively introspected and discussed the customer's challenges in co-ordination with their (customer's) IT Team.

After analyzing the business needs and the expectations of security the solution required by customer, Palo Alto PA-800 Series next-generation firewall appliance was recommended by Wysetek security team. The solutions provided is best fit solution in accordance to client's requirement as security now being the critical component of any organizations. The suggested solution was implemented by the team at the customer end.

Key Benefits

Palo Alto Networks PA-800 Series next-generation firewall appliances comprising of PA-820 and PA-850 are designed to secure enterprise branch offices. The multiple offices of the banking customer could benefit from these models of PA-820 and PA-850 as part of the main next gen firewall offering. PA-800 Series appliances support a wide range of networking features that enable the end user to more easily integrate the security features into their existing network.

PA-800 series is capable of classifying all applications, on all ports, all the time regardless of port, encryption (SSL or SSH) or evasive technique employed. It makes use of application and not the port, as the basis for all of your safe enablement policy decisions and apply traffic-shaping.

PA-800 series can enforce security policies for any user, at any location and deploy consistent policies to local and remote users running on the various platforms such as Windows, Mac OS X, macOS, Linux, Android or Apple iOS platforms. It easily integrates your firewall policies with 802.1X wireless, proxies, network access control and any other source of user identity information.

PA-800 series prevents known and unknown threats and is capable of blocking a range of known threats, including exploits, malware and spyware, across all ports, regardless of common evasion tactics.

Key Benefits of NGFW PA-800 Series Appliance

- Support a wide range of networking features that enable the end user to more easily integrate the security features into their existing network.
- Capable of classifying all applications, on all ports, all the time regardless of port, encryption (SSL or SSH) or evasive technique employed.
- Makes use of application and not the port, as the basis for all of your safe enablement policy decisions and apply traffic-shaping.
- Enforce security policies for any user, at any location and deploy consistent policies to local and remote users running on Windows, Mac OS X, macOS, Linux, Android or Apple iOS platforms.
- Easily integrates your firewall policies with 802.1X wireless, proxies, network access control and any other source of user identity information.
- Prevents known and unknown threats and is capable of blocking a range of known threats, including exploits, malware and spyware, across all ports, regardless of common evasion tactics.