NTIPL's Firewall decision-making process has the ability to understand the details of the Web application traffic passing through it and taking action to block traffic that might exploit vulnerabilities.

Sector and Domain

IT security solutions company

Service & Solution

Palo Alto PA-800 Series

Overview

The company to which we provided the solution is one of the leading IT security solutions company globally. Each product is designed to simplify IT security management across the length and depth of devices and on multiple platforms. They are customized to suit end consumers, small businesses, Government establishments and corporate houses.

Firewall PANW 850

Firewall is a system designed to prevent unauthorized access to or from a private network. They can be implemented in both hardware and software, or a combination of both. Our objective is to build a firewall that blocks unauthorized access while permitting authorized communications using packet filtering.

- 1.9 Gbps firewall throughput[1]
- 780 Mbps Threat Prevention throughput[2]
- 500 Mbps IPsec VPN throughput
- 192,000 max sessions[3]
- 9,500 new sessions per second[3]

- 2,000 IPsec VPN tunnels/tunnel interfaces
- 5 virtual routers
- 40 security zones
- 1,500 max number of policies

Brief Detail about the dilemma

Business was expanding to additional sites; they wanted to ensure that all employees have access to the network resources that they need to be productive. Yet they also wanted to ensure that the network is protected from outside threats. Solution was that sites are connected and ensure security by creating a site-to-site Virtual Private Network (VPN), also called a gateway-to-gateway VPN. A VPN creates a secure tunnel between two sites via the Internet. For example, users at your branch offices can access file servers at the main office. All data is encapsulated so that your confidential information is protected as your users send and receive data.

Solution offered:

- Configured The NAT policy (WAN I)
- Configured address object (Host)
- Then created the services object
- Allowed RDPC (Remote desktop protocol)
- A to B the connection was created using
- WAN (wide area network)

Benefits & solution

Blocks a range of known threats, including exploits, malware and spyware, across all ports, regardless of common threat-evasion tactics employed Limits the unauthorized transfer of files and sensitive data, and safely enables non-work-related web surfing Identifies unknown malware, analyzes it based on hundreds of malicious behaviors, and then automatically creates and delivers protection.

Conclusion

Hence the next generation firewall was implemented successfully