Herve TCHIENKIO

NWIT-245

Prof. Ash Shah

October 5, 2024

**Palo Alto Networks Next-Generation Firewall (NGFW)**

Palo Alto NGFWs utilize deep packet inspection to control traffic based on applications and users rather than just ports or protocols. They come with integrated features like antivirus, anti-spyware, anti-malware, URL filtering, and intrusion prevention systems (IPS), all of which detect and prevent real-time threats. These firewalls support Zero Trust security models, enabling micro-segmentation for granular control over applications, users, and devices. Additionally, they extend security to remote users by protecting endpoints. Palo Alto NGFWs offer impressive performance, delivering throughput from 500 Mbps in smaller models to over 100 Gbps in high-end models. This is crucial for large-scale enterprises. Even with threat prevention and SSL decryption enabled, they maintain low latency. Their support for SSL/TLS decryption is essential in today's heavily encrypted traffic environments. These firewalls scale efficiently, from small businesses to large enterprises, with models that grow alongside network demands. Palo Alto’s seamless cloud integration allows for horizontal and vertical scalability based on workload requirements. The central management platform, Panorama, simplifies managing multiple firewall deployments by providing centralized logging, policy management, and visibility. The intuitive interface has user-friendly dashboards that track traffic, users, and threats. APIs and automation further enhance efficiency in managing complex environments. Palo Alto NGFWs are often deployed in enterprise data centers to secure critical workloads from internal and external threats. They are also used at network perimeters to inspect traffic and block malicious content. Pricing for Palo Alto firewalls varies by model and features. Mid-range models typically cost around $5,000, while high-end models cost $30,000 to $50,000 or more. Implementation times vary based on organization size, ranging from 1-2 weeks for small businesses to several months for large enterprises, particularly when integrated with existing infrastructure. Palo Alto offers VM-series firewalls for virtualized environments like AWS, Google Cloud, and Azure. They also provide Prisma Cloud, a cloud security platform that extends NGFW capabilities to protect workloads, containers, and serverless architectures.