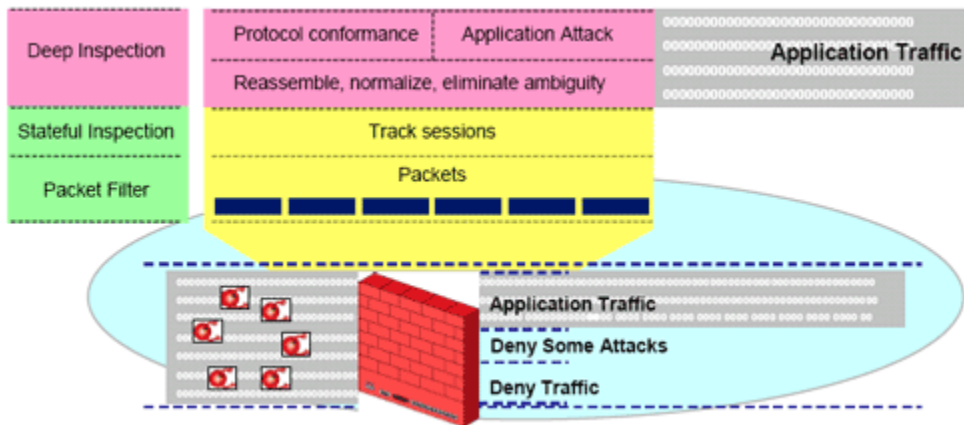


Deep Inspection Firewall

Juniper Networks Deep Inspection firewall builds on the strength of Stateful inspection and integrates intrusion prevention technology into the firewall to provide application-level attack protection at the network perimeter. Leveraging the efficiencies of both technologies, the Juniper Networks Deep Inspection firewall can efficiently perform network security functions as well as analysis on the application message to determine whether to accept or deny traffic.

Juniper Networks Deep Inspection technology applies a deeper level of application understanding to the traffic to make access control decisions based on the intent of that traffic. Deployed at the perimeter, a Juniper Networks Deep Inspection firewall focuses on preventing application-level attacks aimed at Internet-facing applications, NetBIOS, Microsoft Windows, Peer-to-Peer (P2P) and Instant Messaging (IM). It eliminates application-level ambiguities, performing de-fragmentation, reassembly, scrubbing and normalization, to convert network packets to the application-level message being transferred between the client and the server. It then looks for protocol conformance and extracts data from identified application "service fields" where attacks are perpetrated and applies attack pattern matches. It then decides to accept or deny the traffic based on high impact protocol anomalies or any given attack pattern in one of these application service fields. The Deep Inspection firewall can block application-level attacks at the Internet gateway so they never reach their destination.

Additionally, users can also create their own attack protection signatures, leveraging more than 90 available contexts, allowing administrators to detect and pinpoint attacks.



Deep Inspection firewalls can secure the smaller locations in an organization's network that have typically represented the "weak links" in the overall security stance, enabling NetScreen-IDP to focus on detecting the more sophisticated attacks targeted at the larger, more diverse network segments.