**Features and Benefits**

The Palo Alto Networks next-generation firewalls provide granular control over the traffic allowed to access your network. The primary features and benefits include:

**Application-based policy enforcement (App-ID™)—**Access control according to application type is far more effective when application identification is based on more than just protocol and port number. The App-ID service can block high risk applications, as well as high risk behavior, such as file-sharing, and traffic encrypted with the Secure Sockets Layer (SSL) protocol can be decrypted and inspected.

**User identification (User-ID™)—**The User-ID feature allows administrators to configure and enforce firewall policies based on users and user groups instead of or in addition to network zones and addresses. The firewall can communicate with many directory servers, such as Microsoft Active Directory, eDirectory, SunOne, OpenLDAP, and most other LDAP-based directory servers to provide user and group information to the firewall. You can then use this information for secure application enablement that can be defined per user or group. For example, the administrator could allow one organization to use a web-based application but not allow any other organizations in the company to use that same application. You can also configure granular control of certain components of an application based on users and groups (see User Identification).

**Threat prevention**—Threat prevention services that protect the network from viruses, worms, spyware, and other malicious traffic can be varied by application and traffic source (see Objects > Security Profiles).

**URL filtering**—Outbound connections can be filtered to prevent access to inappropriate web sites (see Objects > Security Profiles > URL Filtering).

**Traffic visibility**—Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Application Command Center (ACC) in the web interface identifies the applications with the most traffic and the highest security risk (see Monitor).

**Networking versatility and speed**—The Palo Alto Networks firewall can augment or replace your existing firewall and can be installed transparently in any network or configured to support a switched or routed environment. Multigigabit speeds and a single-pass architecture provide these services to you with little or no impact on network latency.

**GlobalProtect**—The GlobalProtect™ software provides security for client systems, such as laptops that are used in the field, by allowing easy and secure login from anywhere in the world.

**Fail-safe operation**—High availability (HA) support provides automatic failover in the event of any hardware or software disruption (see Device > Virtual Systems).

**Malware analysis and reporting**—The WildFire™ cloud-based analysis service provides detailed analysis and reporting on malware that passes through the firewall. Integration with the AutoFocus™ threat intelligence service allows you to assess the risk associated with your network traffic at organization, industry, and global levels.

**VM-Series firewall**—A VM-Series firewall provides a virtual instance of PAN-OS® positioned for use in a virtualized data center environment and is ideal for your private, public, and hybrid cloud computing environments.

**Management and Panorama**—You can manage each firewall through an intuitive web interface or through a command-line interface (CLI) or you can centrally manage all firewalls through the Panorama™ centralized management system, which has a web interface very similar to the web interface on Palo Alto Networks firewalls.