



Die «Next Generation Firewalls» von Palo Alto setzen auf eine Anwendungs- und User-Kontrolle und steigern dadurch die IT-Security nachhaltig.



«Next Generation Firewalls» machen dicht

Die «Next Generation Firewalls» von Palo Alto basieren auf einer Applikations-, User- und Content-Kontrolle und umgehen so die Begrenzungen herkömmlicher Firewalls mit Port-Kontrolle. Anwendungen und Gefahren lassen sich dadurch einfach identifizieren, transparent darstellen und blockieren.

Konventionelle Firewalls vermögen den aktuellen Gefahren nicht mehr ganzheitlich zu begegnen. So führen etwa Web-basierte Anwendungen wie Skype und Facebook, die Einbindung von Technologien wie Cloud Computing und Virtualisierung oder die mobile Arbeitsweise von Mitarbeitenden dazu, dass sich einzelne User klar definierten IP-Adressen nicht mehr zuordnen lassen. Ebenso wenig sind beispielsweise Web 2.0-Applikationen mit fixen TCP-Ports verbunden; sie lassen sich dadurch nur bedingt kontrollieren.

Diesem Aspekt tragen die «Next Generation Firewalls» (NGF) von Palo Alto Rechnung. Sie setzen auf die Identifikation und Kontrolle von Anwendungen, Benutzern und Inhalten. Dabei werden User unabhängig von IP-Adressen und Applikationen, losgelöst von Port, Protokoll, Verschlüsselung oder Verschleiерungsmethoden erkannt. Dadurch lassen sich Anwendungen und die daraus entstehenden Gefährdungen einfach identifizieren, transparent darstellen und gegebenenfalls blockieren. Palo Alto ermöglicht eine markante Vereinfachung bei der Umsetzung firmenspezifischer Security-Policies. So lässt sich im Rahmen einstufiger Regelwerke komfortabel definieren, welche Anwendungen und

Zugriffe für welche User beziehungsweise Benutzer-Gruppen freigegeben sind, wobei Ports und IP-Adressen vernachlässigt werden können. Relevant sind lediglich die einzelnen Dienste und die userspezifischen Rechte. Demnach gibt Palo Alto nur klar definierte Anwendungen frei (http) und blockiert andere Applikationen, die möglicherweise über Port 80 zu kommunizieren versuchen.

Gefahren einfach erkennen

Die «Next Generation Firewalls» von Palo Alto schaffen ein Maximum an Transparenz. So liefern gut verständliche Reports darüber, was im Netz passiert, welche Anwendungen genutzt werden, welche User mit welchen Programmen beschäftigt sind und wer mit wem kommuniziert. Dank einem umfassenden Realtime-Monitoring erhält der Kunde einen stets aktuellen Überblick über das jeweilige Gefährdungspotenzial. Dazu werden von Palo Alto mehrere Tausend Applikationen erkannt, gefahrenspezifisch eingestuft und – bei deren aktueller Nutzung – visualisiert. Dieser Wert wird stetig aktualisiert und verschafft Security-Managern eine transparente, jederzeit aktuelle Angabe über die momentane Gefährdung sowie über die Verände-

rung des Gefahrenpotenzials im Zeitverlauf.

Ferner verschafft ein übersichtliches «Application Command Center» eine granulare Übersicht über weitere, für die IT-Security relevante Aspekte. Es informiert z. B. darüber, zu welchen Ländern oder geographischen Regionen Verbindungen bestehen, wer im Unternehmen als kritisch eingestufte Applikationen wie Facebook oder Skype nutzt, welcher Datenverkehr durch welche Applikationen erzeugt wird und welche Angriffe am häufigsten vorkommen. Damit auch Grossunternehmen von «Next Generation Firewalls» profitieren, weisen die Lösungen von Palo Alto einen Datendurchsatz im Multi-Gigabit-Bereich auf, überzeugen durch minimalste Latenzzeiten und beeindrucken durch die Fähigkeit, innerhalb eines Zyklus mehrere Analysen parallel zu bearbeiten. □

Kontakt

BOLL Engineering AG

Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch
www.boll.ch

