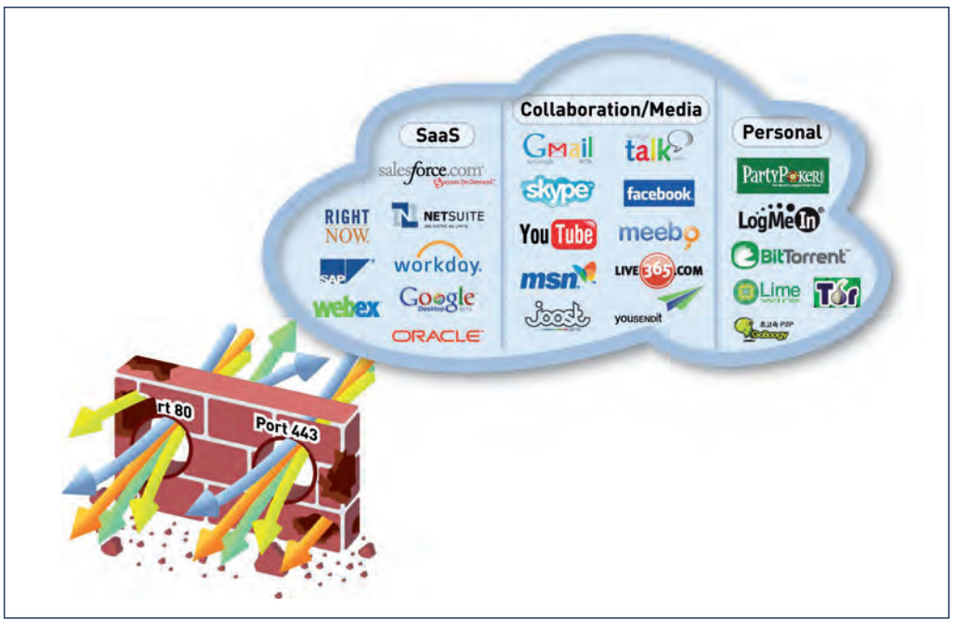
«Next Generation Firewalls» zeigen, was wo läuft

Bisherige Firewalls basieren auf der Kontrolle von IP-Adressen, Ports und Protokollen. Nicht so innovative «Next Generation Firewalls», sie setzen auf eine konsequente Anwendungs- und User-Kontrolle und tragen somit den veränderten Rahmenbedingungen Rechnung.

Es besteht kein Zweifel: Konventionelle Firewalls haben sich zu leistungsstarken Appliances entwickelt, die sich nicht selten durch beeindruckende Durchsatzraten und ein umfassendes «Feature»-Set auszeichnen. Doch dessen ungeachtet rücken die Einschränkungen bisheriger Firewall-Technologien zunehmend ins Blickfeld. Denn selbst die Verknüpfung sich ergänzender Technologien wie Paketfilter, VPN-Gateway, Content-Filter und IDS/IPS vermag den aktuellen Gefahren nicht mehr ganzheitlich zu begegnen. Ob UTM-Appliance oder «Best of Breed»-Gesamtlösung: Die Kontrolle von IP-Adressen, Ports und Protokollen ist und bleibt zwar ein sicherheitsrelevanter Faktor, genügt für eine umfassende IT-Security jedoch nicht mehr. So müssen bei Firewalls unterschiedlichste Ports freigegeben werden – wie beispielsweise Port 80. Was jedoch tatsächlich über die einzelnen Ports kommuniziert wird, lässt sich nur schwer eruieren. Anwendungen wie etwa Skype oder Peer-to-Peer-Programme bilden somit eine perfekte Plattform für Angriffe unterschiedlichster Art.

Die technische Weiterentwicklung der Unternehmens-IT, die vermehrte Nutzung webbasierter Anwendungen wie Skype und Facebook, die Einbindung von Technologien wie Cloud Computing und Virtualisierung oder die vermehrt mobile Arbeitsweise von Mitarbeitenden führen dazu, dass sich einzelne User nicht mehr klar definierten IP-Adressen zuordnen lassen. Ebenso wenig sind beispielsweise Web-2.0-Applikationen mit fixen TCP-Ports verbunden; sie lassen sich dadurch nur bedingt kontrollieren. Vor diesem Hintergrund wird die Kontrolle von Applikationen über Segment- und Perimetergrenzen hinaus mit konventionellen Mitteln schwierig – wenn nicht gar unmöglich. Neue Strategien sind folglich gefragt.



Portblockierende Firewalls können Anwendungen weder sehen noch kontrollieren. «Next Generation Firewalls» hingegen setzen auf eine Anwendungs- und User-Kontrolle und steigern dadurch die IT-Security nachhaltig. Grafik: Palo Alto

Paradigmenwechsel

Eine wegweisende Antwort darauf liefern sogenannte «Next Generation Firewalls», wie sie vom US-amerikanischen Hersteller Palo Alto angeboten werden. Sie läuten einen klaren Paradigmenwechsel im Bereich der Firewall-Technologie ein. Entsprechende Lösungen setzen nicht mehr länger auf die alleinige Kontrolle von IP-Adressen und Port-Nummern, sondern 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 Verschleierungsmethoden erkannt. Dadurch lassen sich Anwendungen und die daraus entstehenden Gefährdungen einfach identifizieren, transparent darstellen und gegebenenfalls blockieren. Wichtig ist dabei, dass die eingesetzte Lösung eine hohe Performance aufweist, um die Sicherheit im Unternehmen nachhaltig zu erhöhen. Gefordert sind unter anderem ein Datendurchsatz im Multi-Gigabit-Bereich, minimale Latenzzeiten und die Fähigkeit, innerhalb eines Zyklus mehrere Analysen parallel bearbeiten zu können.

Der den «Next Generation Firewalls» zugrunde liegende Denkansatz der User- und Applikationskontrolle führt zu wesentlichen Vereinfachungen bei der Umsetzung

DER AUTOR

Walter Benz,
BOLL Engineering

firmenspezifischer Security-Policies. So wird im Rahmen einstufiger Regelwerke komfortabel definiert, welche Anwendungen und Zugriffe für welche User beziehungswiese Benutzergruppen freigegeben sind. Auch in diesem Prozess können Ports und IP-Adressen vernachlässigt werden. 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.
Um die Vorzüge bereits installierter, konventioneller Firewalls mit dem innovativen Ansatz einer «Next Generation Firewall» zu kombinieren, unterstützt Palo Alto eine mehrstufige Integration in jedes beliebige Netzwerk. Dabei ist es möglich, die portbasierten Regeln einer konventionellen Firewall zu übernehmen und mit den applikations- und benutzerbasierten Regeln zu ergänzen – und im Laufe der Zeit gegebenenfalls komplett umzustellen.

«Next Generation Firewalls» setzen auf eine konsequente Anwendungs- und User-Kontrolle.

Bildquelle: Palo Alto

Einfache Erkennung von Gefahren

Aufgrund ihrer user- und anwendungsbasierten Überwachung schaffen «Next Generation Firewalls» ein Maximum an Transparenz. Palo Alto beispielsweise liefert mittels gut verständlicher Reports Informationen darüber, was im Netz passiert, welche Anwendungen genutzt werden, welche User mit welchen Programmen beschäftigt sind und wer mit wem kommuniziert. Dank eines umfassenden Realtime-Monitorings 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 aktuellen Nutzung – visualisiert. Sofern der Kunde die Gefährdung einzelner Applikationen verändern möchte, steht ihm diese Möglichkeit jederzeit zur Verfügung.
Ein übersichtlich gestaltetes «Application Command Center» verschafft einen granularen, transparenten Überblick über die für die IT-Security relevanten Aspekte. Es informiert beispielsweise darüber, zu welchen Ländern oder geografischen Regionen Verbindungen bestehen, wer im Unternehmen als kritisch eingestufte Applikationen wie Facebook oder Skype nutzt oder welche Applikationen am meisten genutzt werden. Viele weitere Informationen lassen sich auf einen Blick erkennen. So zum Beispiel, welcher Datenverkehr durch welche Applikationen erzeugt wird oder welche Angriffe am häufigsten vorkommen. Wünscht der Administrator über einzelne Aspekte detaillierte Informationen, unterstützen ihn automatisch generierte Filter dabei, in Daten hineinzuzoomen und diese genauer zu analysieren.
Für einen schnellen Überblick über den aktuellen Gefährdungslevel errechnet die Security-Plattform auf Basis der jeweils aktiven Applikationen zudem einen Durchschnittswert der Gefährdung. Dieser Wert wird stetig aktualisiert und verschafft Security-Managern eine transparente, jederzeit aktuelle Angabe über die momentane Gefährdung sowie über die Veränderung des Gefahrenpotenzials im Zeitverlauf. <

BOLL Engineering AG
Walter Benz
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch
www.boll.ch

BOLL Engineering: Distributionsvereinbarung mit Palo Alto

Palo Alto Networks wurde im Jahr 2005 durch den Netzsicherheitsexperten Nir Zuk gegründet. Das kalifornische Unternehmen entwickelt innovative «Next Generation Firewalls» für den Enterprise-Markt. Die High-Performance-Systeme basieren auf einer Applikations-, User- und Content-Kontrolle und umgehen somit die Begrenzungen herkömmlicher Firewalls mit Portkontrolle.
Nun hat der IT-Security- und Netzwerk-Spezialist BOLL Engineering mit Palo Alto eine exklusive Distributionsvereinbarung für den Schweizer Markt unterzeichnet. Durch die Partnerschaft komplettiert BOLL sein Lösungsangebot im Netzwerk-Security-Bereich und bietet seinen bestehenden sowie neuen Resellern eine perfekte Ergänzung zum bereits vorhandenen Firewall-Angebot.
Thomas Boll, CEO Boll Engineering, betont den von Palo Alto geschaffenen Mehrwert. «Oft dürften die ‹Next Generation Firewalls› von Palo Alto als ideale Ergänzung zu bestehenden Firewalls eingesetzt werden. Dies nicht zuletzt aufgrund ihrer umfangreichen Visualisierung und ihrer Monitoring-Funktionen. Zudem geben sie dem Administrator leistungsfähige und komfortabel bedienbare Werkzeuge in die Hand. So lassen sich beispielsweise der Traffic länderspezifisch sperren, Videos und Chats personenbezogen blockieren und Applikationen wie Facebook zeitabhängig freigeben.»
Laut Boll sind die Produkte von Palo Alto namentlich für Reseller mit guten Netzwerkkenntnissen und einem klaren Fokus auf Grossfirmen interessant. «Unseren VARs bieten wir ein umfangreiches Dienstleistungspaket an. Dazu gehören eine fundierte Schulung ebenso wie die Begleitung in spezifischen Projekten, Teststellungen und Post-Sales-Support.»