

# Next Generation Firewalls – ein Paradigmenwechsel

Quelle: shutterstock

*Klassische Firewalls basieren auf der Kontrolle von IP-Adressen, Ports und Protokollen. Sogenannte «Next Generation Firewalls» hingegen setzen auf eine konsequente Anwendungs- und User-Kontrolle und tragen somit den veränderten Rahmenbedingungen Rechnung.*

VON THOMAS BOLL

**K**onventionelle 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.

## Identifikation und Kontrolle von Anwendungen, Benutzern und Inhalten

Eine wegweisende Antwort darauf liefern sogenannte «Next Generation Firewalls». 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.

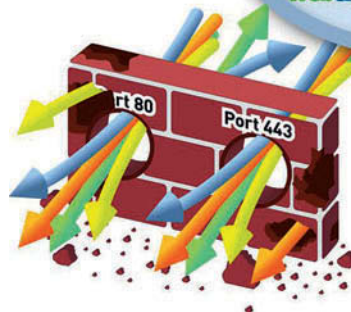
### Neuer Ansatz

Der den «Next Generation Firewalls» zugrunde liegende Denkansatz der User- und Applikations-Kontrolle führt zu wesentlichen Vereinfachungen bei der Umsetzung firmenspezifischer Security-Policies. So wird im Rahmen einstufiger Regelwerke komfortabel definiert, welche Anwendungen und Zugriffe für welche User beziehungsweise Benutzer-Gruppen 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 die «Next Generation Firewall» 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, unterstützen entsprechende Lösungen 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 Re-

*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.*

Quelle: Palo Alto Networks



geln zu ergänzen – und im Laufe der Zeit gegebenenfalls komplett umzustellen.

### Gefahren einfacher erkennen

Aufgrund ihrer user- und anwendungs-basierten Überwachung schaffen «Next Generation Firewalls» ein Maximum an Transparenz. Sie liefern beispielsweise mittels Reports Informationen 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 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 sogenanntes «Application Command Center» verschafft einen granulareren, 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 etwa auch, 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 eine solche 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.

### «Next Generation Firewalls» ergänzen bestehende Security-Appliances

Moderne «Next Generation Firewalls» basieren auf einer Applikations-, User- und Content-Kontrolle und umgehen somit die Begrenzungen herkömmlicher Firewalls mit Portkontrolle. Somit bilden sie oft eine ideale Ergänzung zu bestehenden Firewalls. Dies nicht zuletzt aufgrund ihrer umfangreichen Visualisierung und ihrer Monitoring-Funktionen. Zudem geben sie dem Administrator leistungsfähige und komfortabel bedienbare Werkzeuge in die Hand. ■

Der Autor: Thomas Boll ist CEO der Boll Engineering AG. [www.boll.ch](http://www.boll.ch)



Dank «Next Generation Firewalls» lassen sich Anwendungen und die daraus entstehenden Gefährdungen einfach identifizieren, transparent darstellen und gegebenenfalls blockieren. Quelle: Palo Alto Networks