Haben Sie ein schlechtes Gefühl mit der alten Firewall?

Durch zahlreiche Veränderungen in der Nutzung von Applikationen, dem Nutzerverhalten und der Netzwerkinfrastruktur werden neue Bedrohungslandschaften geschaffen, die Schwachstellen in der portbasierten Netzwerksicherheit offenbaren. Nutzer wollen zunehmend Zugriff auf eine wachsende Zahl von Applikationen über eine große Bandbreite an Gerätetypen hinweg. Dabei machen sie sich in der Regel nur wenig Gedanken über Sicherheitsrisiken für das Unternehmen. Doch die stetige Expansion der Rechenzentren, Netzwerksegmentierung, Virtualisierung und Mobility-Initiativen erfordern ein Umdenken bei der Verwendung von Applikationen und Daten. Gleichzeitig steht der Schutz des Unternehmensnetzwerks vor neuen Herausforderungen wie höher entwickelte Advanced Threats, die herkömmliche Sicherheitsmaßnahmen umgehen können.

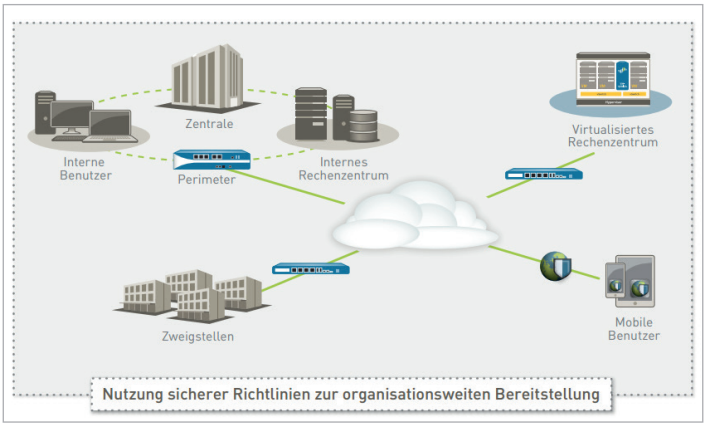

Abbildung 1: Nutzung sicherer Richtlinien

Funktionsweise

Statt wie bei herkömmlichen port-basierten Firewalls wird bei einer Next Generation Firewall (NGFW) nicht nur einfach auf IP-Adresse und Port geschaut (Layer3), sondern es wird bis zum Layer 7 (Applikation) analysiert. Hierdurch ist es möglich, sehr granular zu unterscheiden, ob über Port 80 nur eine Webseite aufgerufen oder Peer-to-Peer gemacht wurde. Zu diesem Zweck wurde von Palo Alto Networks die Single-Pass Parallel Processing (SP3) Architektur entwickelt.

Jedes Paket nimmt hierfür genau den selben Weg (Single-Pass) und wird durch mehrere Stufen der Erkennung geführt. Als erstes wird anhand der IPs/Ports analysiert, ob es eine Security Policy gibt, die diesen Traffic überhaupt erlaubt. Nur wenn diese gefunden wird, wird das Paket genauer untersucht. In dieser Analyse erfolgt nun die Bestimmung der Applikation, wie z. B. Web browsing. Wird in diesem Schritt festgestellt, dass die Applikation SSL (also verschlüsselter Traffic) ist, wird automatisch geprüft, ob es für diese Verbindung eine passende Decryption-Regel gibt. Ist dies der Fall, wird der Verkehr transparent entschlüsselt und die Applikation erneut geprüft. Die Erkennung der Applikation erfolgt in zwei Stufen.

In der ersten Stufe werden Signaturen angewendet, um die Anwendung anhand von einzigartigen Eigenschaften und zugehörigen Transaktionsmerkmalen zu erkennen. In der zweiten Stufe werden dann Decoder für bekannte Protokolle angewendet, um zusätzliche kontextbasierte Signaturen auf die Applikation anzuweden, die durch das Protokoll getunnelt wurden (z. B. Facebook über HTTP). So wird die innenliegende Applikation detektiert. Für Applikationen, die nicht durch eine erweiterte Signatur- und Protokollanalyse erkannt werden können, werden Heuristicen angewandt, um die Anwendung zu erkennen. Nach der Erkennung der Applikation wird überprüft, ob eine Sicherheitsregel vorhanden ist, die diesen Verkehr erlaubt bzw. blockiert.

Im nächsten Schritt wird nun versucht, die IP-Adresse mit einem Benutzer (User-ID) in Verbindung zu bringen. Hierbei kann über verschiedene Wege eine bestehende Infrastruktur (Microsoft AD, Radius, Microsoft Exchange usw.) abgefragt werden. Diese Informationen fließen mit in die Auswertung für spätere Analysen oder werden direkt in den Sicherheitsregeln benutzt. Damit kann eine Regel nur für eine Person oder für eine Gruppe definiert werden.

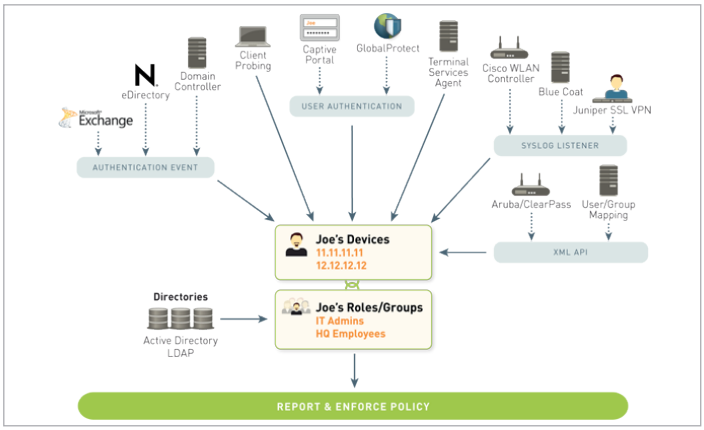

Abbildung 2: Rollenvergabe bei Palo Alto Networks. Quellen für User-ID Informationen (Mapping User-to-IP)

Im letzen Schritt wird noch der Inhalt der Verbindung (Content-ID) überprüft. Diese Überprüfung teilt sich in drei Hauptkategorien auf. Die erste ist ein integrietes IPS mit zugehörigem Anti-Malware-Schutz. Das IPS schützt vor Exploits von bekannten Sicherheitslücken, Pufferüberlauf, DoS-Angriffen und Port-Scans. Zusätzlich werden auch ungültige oder fehlerhafte Pakete gefiltert und IP-Defragmentierung und TCP-Remontage unterbunden.

Durch eine signaturbasierte Datenanalyse des Verkehrs wird eine Antivirusprüfung durchgeführt. Diese Analyse erfolgt in-line mit einem sehr hohen Durchsatz und kann auf die Protokolle HTTP, SMTP, IMAP, POP3, FTP und SMB angewandt werden. Durch eine fortlaufende Analyse des Verkehrs durch die Anti-Spyware wird die Spyware/Malware-Kommunikation erkannt und gestoppt.

Die zweite Kategorie ist die URL-Filterung. Weitere Informationen hierzu finden sich auf dem Datasheet zum Thema Palo Alto Networks URL-Filter (Web & E-Mail Security).

Die letzte Kategorie enthält die Datei- und Datenfilterung. Bei der Dateifilterung kann definiert werden, welche Dateitypen geblockt werden sollen. Ein Download einer .exe wäre z. B. nicht erlaubt, ein .pdf allerdings schon. Zusätzlich kann auch definiert werden, dass der Anwender beim Download eine Warnseite angezeigt bekommt und erst nach einem bewussten Klick auf den Continue Button der Download wirklich ausgeführt wird. Dadurch wird ein Drive-by-Download unterbunden. Über die Wildfire Analyse kann ein Download (aus dem Internet) zur Analyse an die Wildfire Cloud (public oder private) übermittelt werden.

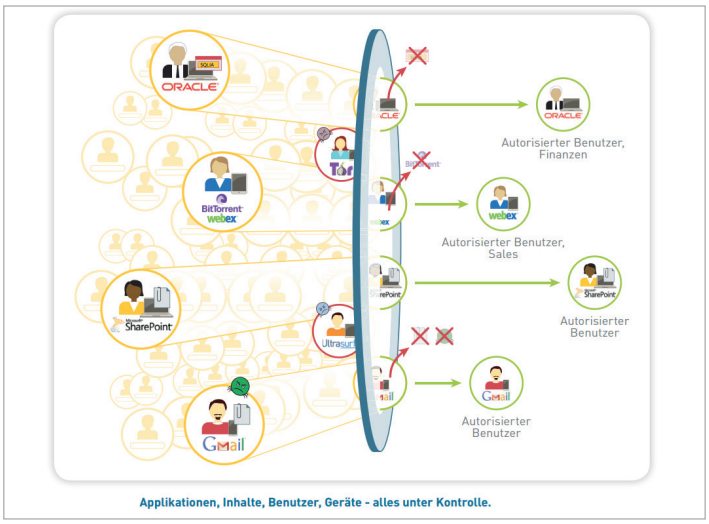

Abbildung 3: Filterung der Dateitypen

Über die Datenfilterung kann eine einfache DLP (Data Loss Prevention)-Lösung implementiert werden. Hierbei scannt die Engine auf Muster innerhalb von Dokumenten und blockiert die Verbindung bei einer Überschreitung von Schwellwerten.

All diese Stufen durchläuft jedes Paket, hierdurch kann auch ein Wechsel der Applikation innerhalb einer Verbindung erkannt werden und die Überprüfung, ob es eine Sicherheitsregel gibt, erneut durchgeführt werden.

Architekturmodell

Die Enterprise Security Plattform von Palo Alto Networks ist als Hardware- sowie visualisierte Plattform verfügbar. Die speziell entwickelte Hardware-Plattform ist vom kleinen Zweigbüro bis hin zum Rechenzentrum vollständig skalierbar. Die virtualisierte Plattform dient der Unterstützung Ihrer Cloud Computing-Initiativen.

Palo Alto Networks unterstützt die größte Bandbreite an virtuellen Plattformen, um Ihre jeweiligen Anforderungen an virtualisierte Rechenzentren ebenso wie an öffentliche und private Cloud-Umgebungen zu erfüllen. Die Firewall-Plattform der VM Series ist für VMware ESXi, NSX, Citrix SDX, Amazon AWS, und KVM Hypervisors erhältlich. Egal ob Sie Ihre Plattformen physisch oder virtuell einsetzen, Panorama kann immer für das zentrale Management genutzt werden. Hierbei handelt es sich um ein optionales Angebot für ein zentrales Management mit dem Sie Transparenz über Traffic-Muster erhalten, Richtlinien umsetzen, Reports erzeugen und Content-Updates zentral bereitstellen können.

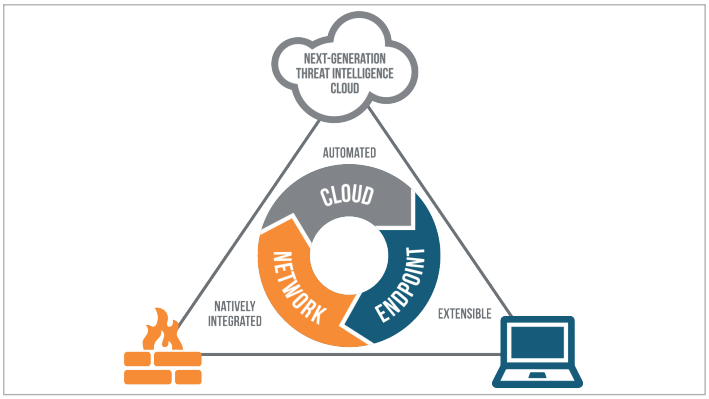

Abbildung 4: Architekturmodell

Leistungen

Die Experten der iT-CUBE planen und installieren mit Ihnen zusammen Ihre neue Next Generation Firewall. Zusätzlich integrieren wir alle nötigen 3rd Party-Komponenten wie Proxy, VPN-Gateways oder IPS. Besitzen Sie bereits ein SIEM bzw. Log Management System, integrieren wir die Lösung in diese. Darüber hinaus helfen wir beim Aufbau eines zentralen Managements.

Nutzen

Unsere Mitarbeiter sind zertifizierte Palo Alto Networks Accredited Sales Experts und Certified Network Security Engineers und Teil des Palo Alto Network Authorized Support Center.

Unsere Experten haben bereits viele Projekte mit unterschiedlichsten Produkten erfolgreich umgesetzt. Wir nutzen diese jahrelange Erfahrung, um die NGFW von Palo Alto Networks perfekt in Ihre bestehende Infrastruktur zu integrieren. Firewall-Systeme können etwa genutzt werden, um einzelne Systeme oder ganze Abteilungen zu seperieren.

Die Mitarbeiter von iT-CUBE stehen im engen Kontakt mit Palo Alto Networks. Dadurch können technische sowie organisatorische Probleme schnell und reibungslos gelöst werden. Schon kurz nachdem Palo Alto Networks den europäischen Markt betrat, starteten wir bereits mit gemeinsamen Projekten durch.

Um Sie besser auf Sicherheitsvorfälle und den Umgang mit der Lösung zu schulen, bietet iT-CUBE speziell auf Ihre Bedürfnisse zugeschnittene Workshops für Ihre Mitarbeiter an.

iT-CUBE SYSTEMS AG

Paul-Gerhardt-Allee 24
81245 München, Germany

T: +49 89 2000 148 00
F: +49 89 2000 148 29

info@it-cube.de
www.it-cube.de