



ANDREAS MERTZ

Next Generation Firewalling - Kontrolle von Applikation, Inhalt und Nutzer

Schwierigkeitsgrad:



Spätestens nach der Analyse verbreiteter Anwendungen wie Skype™, WebEx™ oder GBridge™, wird eines klar: Applikationen haben sich verändert - Paketfilter nicht. Mit einer klassischen Paketfilter-Firewall verlieren die Security-Abteilungen zunehmend die Kontrolle über den Perimeter.

Web2.0-Applikationen, die neue Mobilität sowie neue Bedrohungsarten haben die Aufgabe des traditionellen Paketfilters, immer unwichtiger werden zu lassen. Der Trend, einzelne Bedrohungsrisiken durch dedizierte Lösungen wie Intrusion Prevention Systeme (IPS), Content Filter (Application Level Gateways, Proxies), Web Viren Scanner, Instant Messaging Filter, etc. abzusichern, ist ungebrochen. IT-Abteilungen stöhnen unter der Last, die Komplexität, Betriebsaufwand sowie Support-/ Maintenance-Kosten mit sich bringen. Dennoch sind sie nicht in der Lage, den Fluss moderner Applikationen über Segment- und Perimetergrenzen hinweg wirksam und Policy-konform abzusichern.

Betrachtet man die Veränderungen in der Applikationslandschaft, wird eines klar: Etliche Anwendungen aus dem privaten Sektor halten Einzug in die geschäftliche Nutzung; angefangen von Instant Messaging (IM) bis hin zu geschäftsrelevanten Web2.0-Anwendungen, auch Enterprise2.0-Anwendungen genannt. Zweifelsohne verändert sich die Verkehrsmatrix durch IM, Blogging, Cloud-based Computing, Collaboration, Social Networking usw., die nach [1] bereits 38% an der Gesamtzahl typischer Anwendungen im Geschäftsleben ausmachen.

Ein weiterer Aspekt vieler neuer Webapplikationen sind deren Servereigenschaften. Auf PC oder Notebook, auf denen bisher Client-Anwendungen ausgeführt wurden, laufen mittlerweile etliche Serverdienste, u.a. als mobiler Code im Browser.

Viele Applikationen werden zu Lasten der Sicherheit vorrangig auf Funktion und Connectivity getrimmt. Sie nutzen dafür Techniken, mit denen IT-Sicherheitssysteme gezielt umgangen werden können und adaptieren sich an die Umgebung. Beispielsweise starten sie für den Verbindungsaufbau mit der Verwendung einer Sequenz, typischerweise an der Firewall offener UDP- und TCP-Ports, sind Proxy-fähig oder verfügen selbst über Proxy-Funktionen (z.B. Skype). Andere Anwendungen wechseln dynamisch von http auf https oder proprietäre Verschlüsselungsverfahren, wenn sie blockiert werden. Häufig anzutreffen ist auch die *Webifizierung*, d.h. die Anwendung kommt auf Basis mobiler Codes im Web-Browser zur Ausführung und entzieht sich so der Kontrolle durch Management-Tools für Client-Software.

Nun stellen Applikationen als solche noch keine Bedrohung dar. Leider bergen sie aber enorme Risiken, weil durch den Übergang vom gesicherten LAN in die Internet-Cloud die Kontrolle sehr schwierig wird. Mehr als 70% der Enterprise2.0-Anwendungen beinhalten Filetransfer-Funktionen. Sie begünstigen damit den unkontrollierten Informationsabfluss und setzen die Hürden für Industriespionage herab. Bei anderen Beispielen verschwimmt die Grenze der privaten und geschäftlichen Nutzung und begünstigt den Einzug der „Click-now-think-later“-Mentalität.

HTTP – das neue TCP/IP?

Das eben Genannte hat signifikante Auswirkungen zur Folge: Ein User entspricht nicht mehr einer

IN DIESEM ARTIKEL ERFAHREN SIE...

Warum klassische Paketfilter nicht mehr greifen;

Welche Kernanforderungen eine neue Firewall-Generation erfüllen muss;

Welche technischen Konzepte am Beispiel einer Palo Alto Networks Firewall nötig sind.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN...

Firewalling, Content Security, Intrusion Prevention.

IP-Adresse und Applikationen können oftmals TCP-/UDP-Ports nicht mehr fest zugeordnet werden. Ein Blick auf die Firewall verdeutlicht den Kontrollverlust: Obgleich vor allem am Perimeter nur wenige offene Ports in Richtung Internet (z.B. TCP 80, 443, 25, 53, 123, ...) existieren und in eingehender Richtung, wenn überhaupt, nur Port 25 geöffnet ist, können etliche Applikationen ungehindert passieren. Anders formuliert kann http/https als das neue TCP/IP bezeichnet werden.

Spätestens jetzt wird klar, dass die alten Denkschemata des Stateful Packet Inspection ausgedient haben. Die Security-Abteilung ist nicht mehr in der Lage, den Fluss von Applikationen über Segmentgrenzen und Perimeter hinweg sicher zu kontrollieren.

Kaum eine Organisation setzt heute am Perimeter ausschließlich Paketfilter ein. Die Sinnhaftigkeit eines Einsatzes von Netzwerk-basierten IDS/IPS (NIDS/NIPS) am Perimeter dürfte mittlerweile häufiger in Frage gestellt werden, wenn an den technisch möglichen Integrationspunkten überwiegend verschlüsselter Datenverkehr keine effektive Angriffserkennung mehr zulässt. Die Protokolle HTTP, HTTPS und FTP werden in der Regel durch Web-Proxies mit Content Scanner und URL-Filterfunktionen abgesichert. Web-Proxies greifen auf Verzeichnisdienste zu (z.B. ActiveDirectory oder LDAP) und ermöglichen so benutzerbezogene Regelwerke für den Internetzugriff. Betrachtet man die Funktionsweise aktueller Web-Proxies aber genauer, so ist festzustellen, dass auch sie kaum in der Lage sind, Web2.0-Applikationen sicher zu erkennen, geschweige denn auf funktionaler Ebene zu filtern. Eine Übertreibung? Keineswegs! Salesforce™ und WebEx™ vollständig zu blockieren, dürfte unter den Anwendern kaum Zustimmung finden.

Was sich in den letzten fünf Jahren als technische Antwort auf Bedrohungen etabliert hat, war das *Übereinanderstapeln* von unterschiedlichen Systemen: Paketfilter, VPN-Gateway, Application Level Gateway/Content Filter, IDS/IPS, Web-Virus-Scanner, etc. Das Ergebnis: hohe Komplexität, vier, fünf, und mehr komplett unterschiedliche GUIs; keine Cross-Device-Eventkorrelation, unerwünscht hohe

Latenzzeiten, ressourcenintensiver operativer Betrieb.

Auch Unified-Threat-Management-Ansätze (UTM), die es seit mindestens 5 Jahren gibt, haben nicht viel geholfen. Wenn sich hinter dem funktionsgeladenen GUI ein Architekturmodell verbirgt, das lediglich den Verkehr durch verschiedene Filter-/Analysemodule hindurch schleift, stellt das keine echte Integration dar. Insbesondere UTM-Ansätze, die auf Open Source Modulen aufsetzen, kranken sehr oft an diesem Architekturfehler und büßen zudem ihre Enterprise-Tauglichkeit durch zu hohe Latenz und mangelhafte Stabilität ein.

Kommen wir noch einmal zurück zum Beispiel WebEx™, einem typischen Vertreter sogenannter Collaborative Tools, der sich, gerade in IT-Kreisen, großer Beliebtheit erfreut. Die Teilnahme an Webkonferenzen ist zweifelsohne ein Muss.

Schwieriger wird es schon zu begründen, warum ein Mitarbeiter Funktionen wie Desktop Sharing und Filetransfer nutzen muss. Genau an dieser Stelle liegt das Manko aller klassischen Sicherheitslösungen: Sie sind nicht in der Lage, Applikationen sicher zu erkennen und unerwünschte bzw. unsichere Funktionen zu filtern.

Die Firewall ist tot. Es lebe die Firewall!

Frisches Denken im Firewalling ist gefordert. Die zentralen Anforderungen an eine echte „Next Generation“ lassen sich einfach ableiten:

- Identifikation von Applikationen unabhängig von Port, Protokoll, Verschleierrungsmethoden oder Verschlüsselung
- Identifikation von Benutzern unabhängig von der IP-Adresse

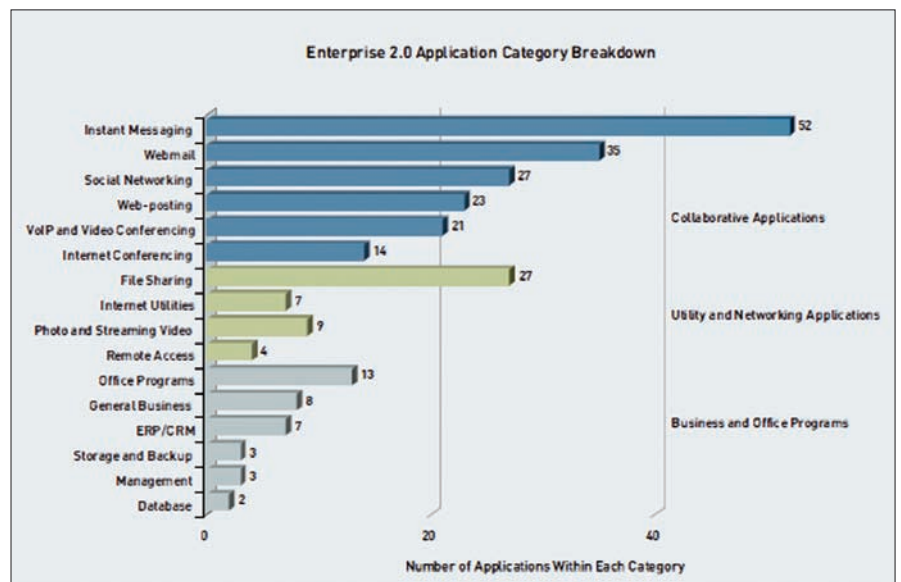


Abbildung 1. Überblick Enterprise 2.0-Applikationen (Quelle [1])

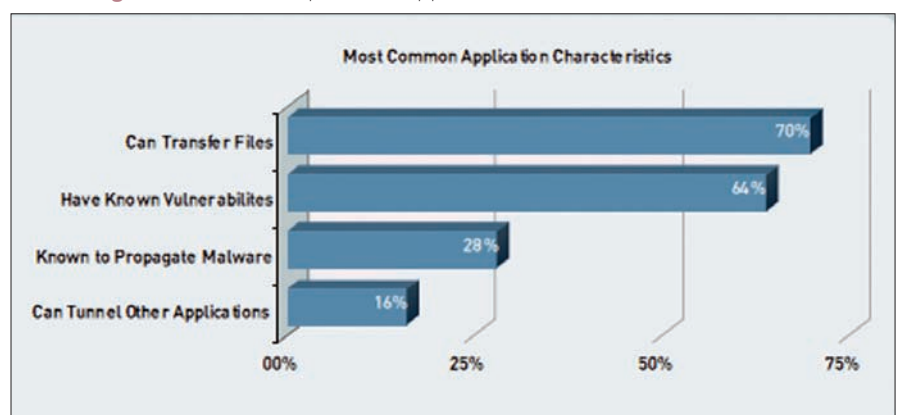


Abbildung 2. Geschäfts- und Sicherheitsrisiken in Web2.0-Anwendungen (Quelle [1])

FÜR EINSTEIGER

- Granulare Sicht und Kontrolle über Anwendungszugriffe und Funktionen
- Echtzeitschutz gegen in Anwendungen versteckte Bedrohungen
- Multi-Gigabit-Durchsatz, In-line Integration, minimale Latenzerhöhung

zer und der Inhalte in sich vereinigen. Er muss, wenn Multi-Gigabit-Durchsatz, In-line Integration und minimale Latenzerhöhung eine Kernanforderung ist, auf einer massiv-parallel arbeitenden Prozessorarchitektur aufbauen, um innerhalb eines Zyklus mehrere Analysen gleichzeitig abzuwickeln. Das System muss für Änderungen flexibel bleiben, spricht auf einem FPGA-Design

beruhen, und Daten- und Kontrolleinheiten strikt trennen.

Wirft man einen Blick auf die aktuellen Angebote der traditionellen Firewall-Hersteller, setzt Ernüchterung ein. Fast alle haben verschlafen. Hoffnung keimt in den neuen, innovativen Startups und ihren Vordenkern. Als Beispiel sei hier Nir Zuk genannt, Mitentwickler der Stateful Inspection

Ein neuer Lösungsansatz muss also die Identifikation der Anwendung, der Benut-

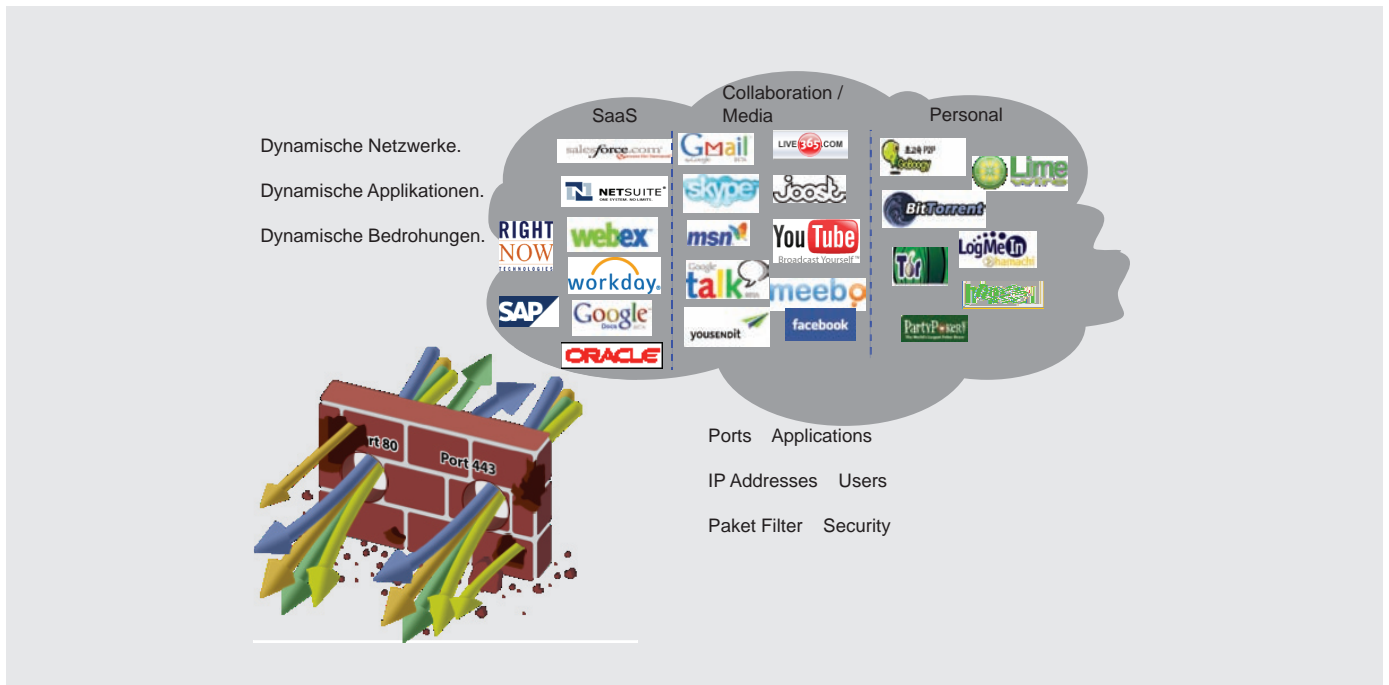


Abbildung 3. Kontrollverlust am Perimeter

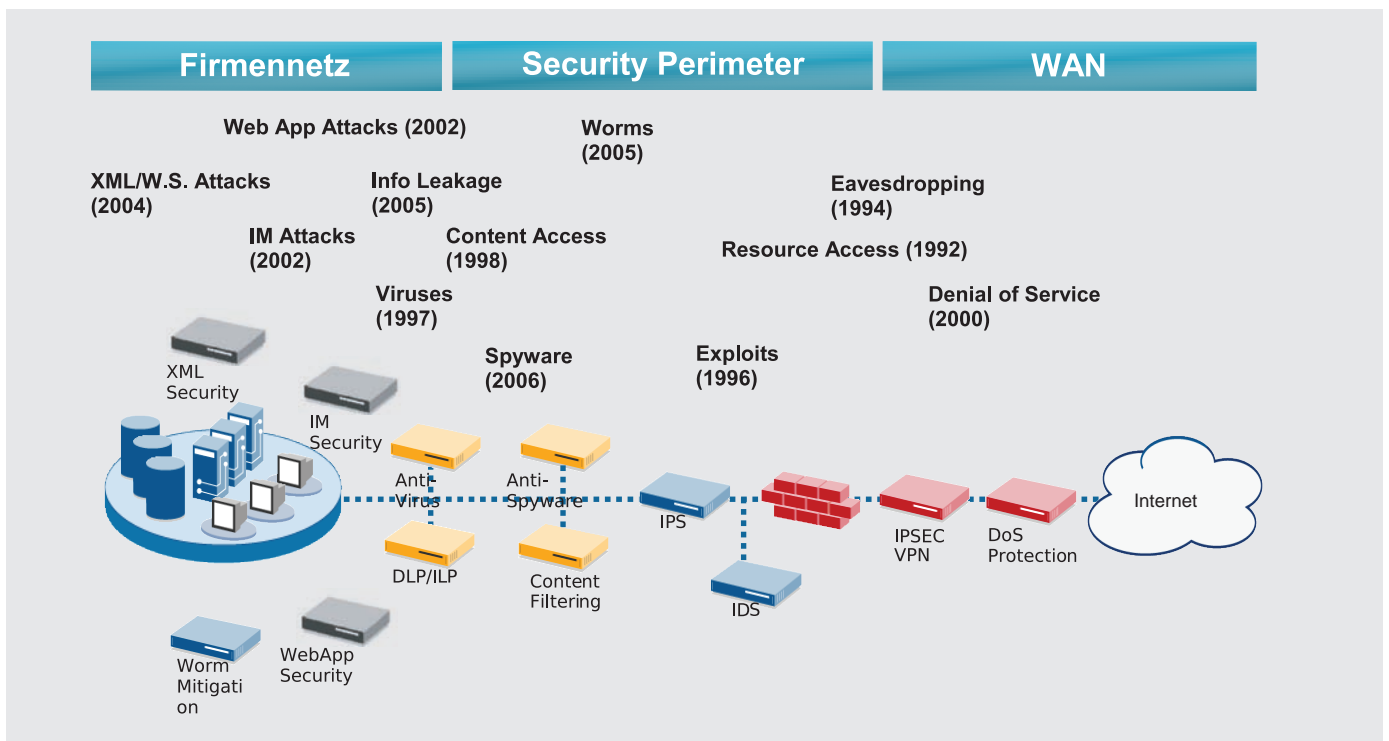


Abbildung 4. IT-Security Infrastruktur 200x

Firewall Technologie bei Check Point™, Gründer von OneSecure, einem Pionier der Intrusion Prevention und Detection Appliances und später CTO bei NetScreen™ Technologies, welches 2004 von Juniper Networks übernommen wurde, der Firewalling neu definiert hat. Seine Palo Alto™ Appliances verwirklichen einen tragfähigen Ansatz, mit dem Applikationen unabhängig vom genutzten Port und darüber hinaus auch User und Content erkannt und kontrolliert werden können. Die Systeme entschlüsseln HTTPS-Verkehr *on the fly* und sind in der Lage über 800 Applikationen zu

erkennen, deren Verhalten zu interpretieren und diese ganz oder auf Funktionsebene zu filtern. Das stellt eine neue Qualität dar und ist uns Grund genug, das System etwas näher unter die Lupe zu nehmen.

Palo Alto Networks – Eine echte Next Generation Firewall?

Um 800 Applikationen filtern zu können, musste für die Palo Alto™ Next Generation Firewall (PAN) ein neues Architekturmodell von Grund auf konzipiert werden. Eine sogenannte „Single Pass Parallel Processing

(SP3) Architecture“ bildet die Grundlage für den hohen Durchsatz und die geringe Latenz bei gleichzeitiger Verbesserung der Applikations- und Datenanalyse. Im Gegensatz zu herkömmlichen, meist Intel-basierten Security Geräten, setzt sie auf FPGAs und parallel arbeitende Prozessoren. Die Architektur basiert im Kern auf zwei Säulen: der Single Pass Software und der Parallel Processing Hardware.

Das Ziel der Single Pass Software ist es, jede Operation nur ein Mal pro Paket durchzuführen. Wenn ein Paket verarbeitet wurde, sind die Aufgaben der Netzwerk-

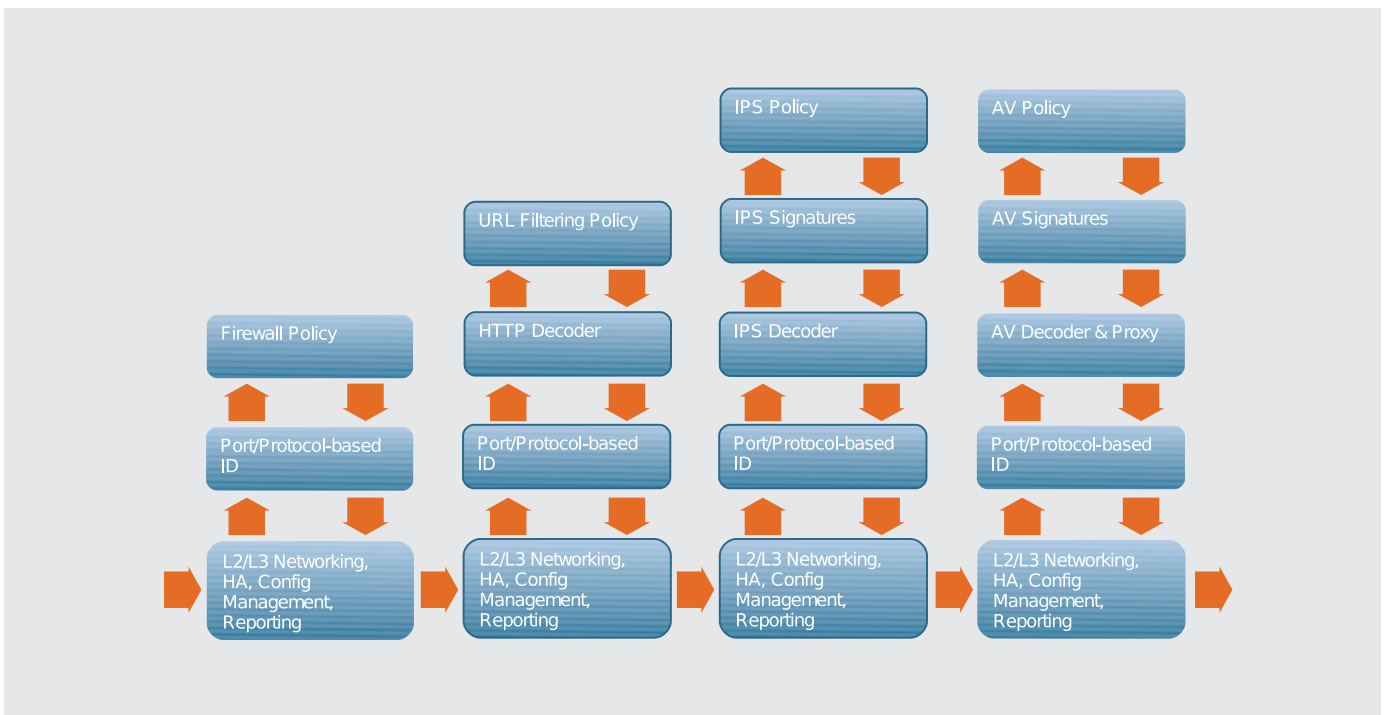


Abbildung 5. Generisches UTM-Architekturmodell



Abbildung 6. Next Generation Firewalling - Anforderungen

FÜR EINSTEIGER

ebene, Regelwerksanalyse, SSL-Ent-/ Verschlüsselung, Applikationsidentifizierung sowie die Signaturanalyse für alle Angriffe und alle Inhalte in einem Schritt durchgeführt worden. Dies reduziert den Arbeitsaufwand verglichen mit UTM-Systemen, die jede Funktion einzeln abarbeiten, enorm. Zum Anderen ist die Inhaltsanalyse der Palo Alto Networks™ Single Pass Software tatsächlich Stream-basiert und nutzt identische Signaturen zur Erkennung

von Angriffen und Viren. Dadurch wird die Latenz extrem gering gehalten. Im Gegensatz dazu müssen Proxies und UTM-Systeme i.d.R. die Daten erst komplett herunterladen und für jede Analyse eine eigene Engine mit eigenen Signaturen nutzen. Dass Pakete mehrfach gescannt werden.

Um eine hohe Performance der Single Pass Software zu ermöglichen, wurde die Hardware parallelisiert. Die Verarbeitung

des Verkehrs wurde vom Management der Firewall komplett getrennt. Für das FW-Management kommt ein separater Prozessor zum Einsatz. Ebenso sind die Speichereinheiten, um die Protokolldaten zu speichern, zu analysieren und Berichte zu erstellen oder die Regeln und Konfiguration des Systems zu verwalten, abgetrennt worden.

Auf der Datenebene wurden die Aufgaben für die Verarbeitung spezialisierten Komponenten überlassen. Routing, Flow Lookup, Stats Counting, NAT und Ähnliches werden durch den Netzwerkprozessor übernommen. User-ID, App-ID und Regelwerksanalyse wird von einer Multi-Core Security Engine mit Hardwarebeschleunigern für Ver- und Entschlüsselung und Dekomprimierung durchgeführt. Die Inhaltsanalyse nutzt eine Flash Matching Engine, um die Daten schnell und sicher zu identifizieren und zu analysieren.

Basierend auf dem Security-Betriebssystem PAN-OS™ kombinieren Palo Alto Networks™ Appliances die bereits genannten vier Technologien: Applikationskontrolle (App-ID™), Integration der Benutzeridentität (User-ID™), Content Filtering (Content-ID™) sowie Networking, IPSec-VPN und Managementfunktionen:

App-ID™

App-ID erkennt Applikationen und je nach Anwendung auch einzelne Funktionen

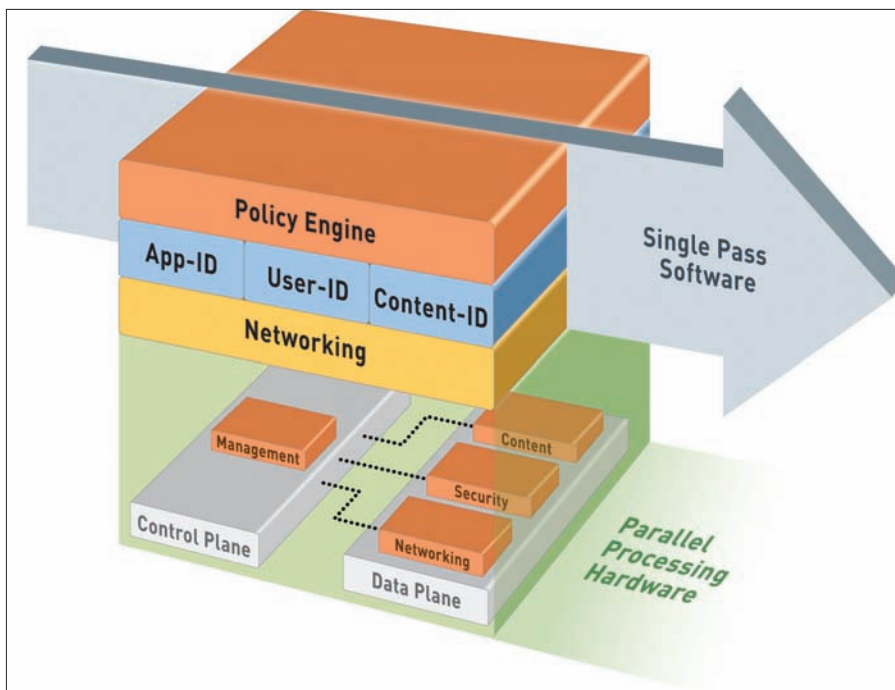


Abbildung 7. Prinzipdarstellung: PAN-Architektur (Quelle [2])

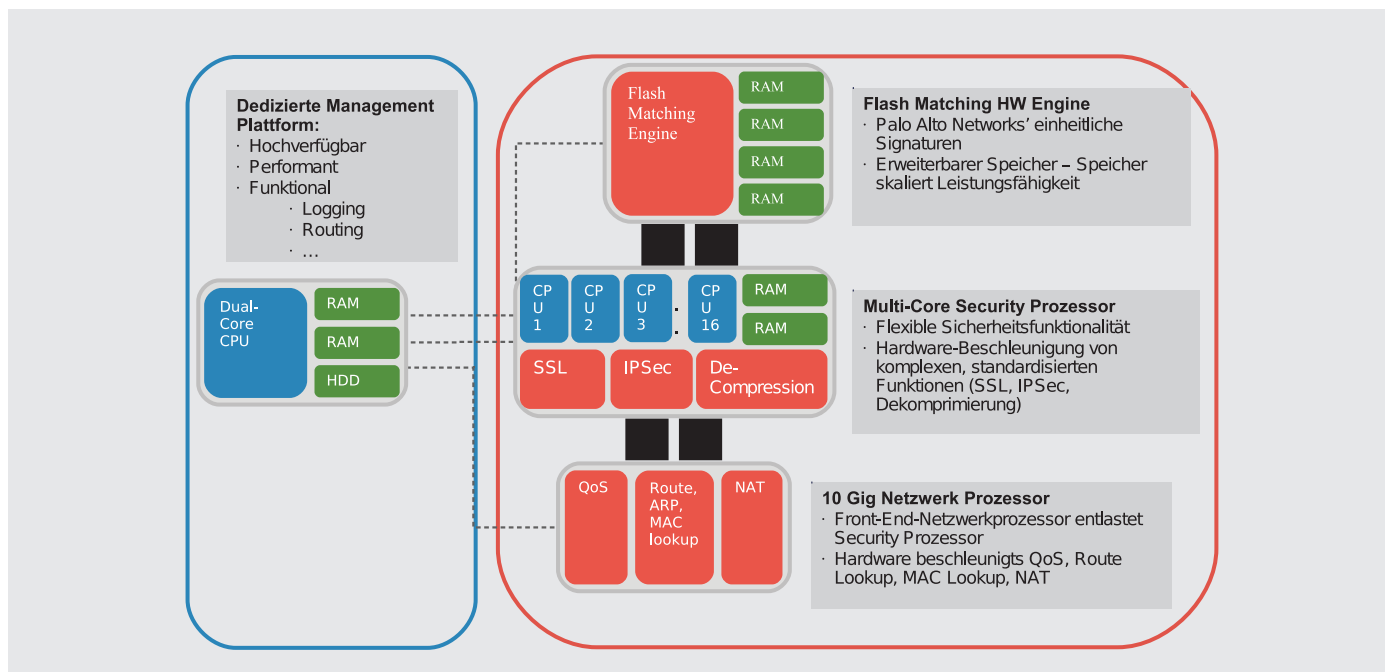


Abbildung 8. PAN-Systemarchitektur PA4000 (Quelle [2])

FÜR EINSTEIGER

innerhalb einer Applikation, unabhängig von dem verwendeten Port. Dies geschieht vor allem mit Hilfe von Applikationsprotokollererkennung und -entschlüsselung, Applikationsprotokolldekodierung, Applikationssignaturen und Heuristiken.

SSL-Entschlüsselung

Mit der Applikationsentschlüsselung ist es möglich, Verbindungen von Benutzern auf Webseiten zu kontrollieren, die durch SSL geschützt sind. Natürlich kann man diese Entschlüsselung für bestimmte Kategorien von Webseiten deaktivieren, z.B. für Homebanking oder Krankenkassen, um die gesetzlichen Vorgaben aus dem Arbeitsrecht zu erfüllen.

In umgekehrter Verkehrsrichtung kann der eigene Webserver vor Angriffen geschützt werden, indem SSL-Verbindungen aufgebrochen und durch die Real Time Threat Prevention z.B. vor SQL Injections oder Brute Force Attacks geschützt werden.

User-ID™

Haben Sie schon einmal versucht, eine Applikation nur für bestimmte Benutzer an einer Firewall freizuschalten während die Benutzer ihre IP-Adressen dynamisch per DHCP zugewiesen bekommen? User-ID basiert auf einem Agenten, der die Zuordnung von IP-Adressen zu Benutzern aus dem Si-

cherheitsprotokoll des Domain Controllers extrahiert und diese Informationen der Palo Alto Networks™ Firewall mitteilt. Benutzer ohne Active Directory Anmeldung können sich über ein Captive Portal an der Firewall identifizieren. Einzelne Benutzer oder Gruppen können aus dem Active Directory ausgelesen und im Regelwerk als *Quelle* verwendet werden.

Content-ID™

Die Content-ID Technologie basiert auf mehreren Techniken. Eine der Schlüsseltechnologien für Content-ID ist die Hauptklassifizierungskomponente von App-ID, die Applikationsprotokolldekodierung. Content-ID verwendet den reassemblierten Applikationsdatenstrom der Applikationsprotokolldekodierung und prüft diesen auf Angriffs- oder Data Leakage-Muster, dafür kommt ein integriertes IPS zum Einsatz. Die Stream-basierte Virus Scanning Technologie beginnt das Scannen schon beim ersten ankommenden Paket einer Datei und wartet nicht ab, bis erst die ganze Datei im Speicher vorhanden ist. Damit lassen sich Performance- und Latenzprobleme auf ein Minimum reduzieren.

PAN im Betrieb

Schon der erste Blick auf die GUI lässt ahnen, dass die besten Ansätze aus Check Point™, Juniper™ und anderen Produkten

aufgegriffen und weiterentwickelt wurden. Durch ein kombiniertes Regelwerk ist es möglich, die Port-basierten Regeln einer traditionellen Firewall zu übernehmen und diese durch Benutzer- und Applikationsbasierte Regeln zu ergänzen und mit der Zeit langsam umzustellen.

Palo Alto Networks™ Next Generation Firewall lässt sich in jedes beliebige Netzwerk integrieren. Im einfachsten Fall fängt man an, die Next Generation Firewall an einen passiven Port (SPAN-Port) des Netzwerkes anzubinden, um die benutzten Applikationen im Datenstrom zu analysieren. Im nächsten Schritt kann man die Firewall im Layer 2 Modus transparent in das Netzwerk einbringen. Besonders interessant hierbei ist der Virtual Wire Modus, bei dem die Firewall noch nicht einmal eine MAC-Adresse besitzt und die Daten nur von einem zum anderen Interface weiterleitet und dabei kontrolliert. Im traditionellen Layer 3 Modus kann man alle Features der Firewall voll nutzen. Dazu werden dynamische Routingprotokolle wie RIP v2, OSPF und BGP unterstützt. Durch die große Anzahl von zur Verfügung stehenden Netzwerkanschlüssen und die flexiblen Konfigurationsmöglichkeiten der Palo Alto Networks™ Next Generation Firewall ist es ebenfalls möglich, alle 4 beschriebenen Betriebsarten kombiniert zu nutzen.

Quellen:

- [1] Application Usage & Risk Report, Fall 2009, Palo Alto Networks
- [2] Palo Alto Networks Inc., 2010

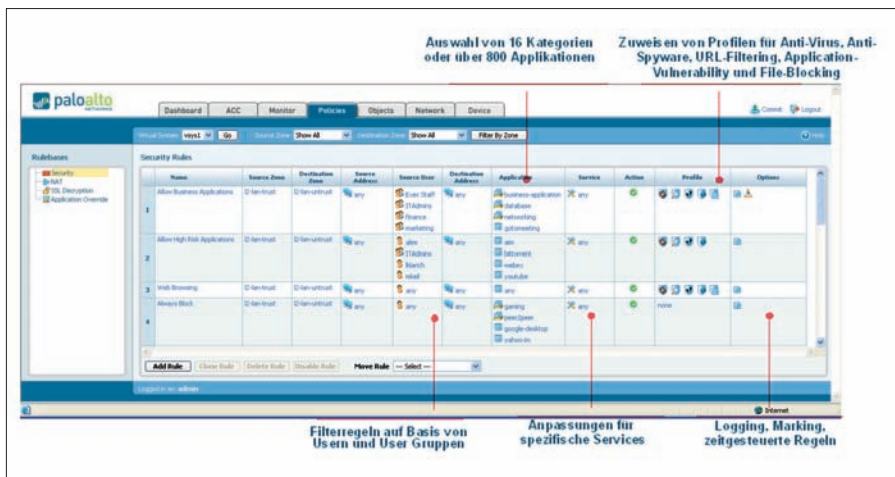


Abbildung 9. PAN-GUI

Fazit

Mit dem Einzug von Web2.0-Applikation müssen IT-Security-Abteilungen ihre Sicherheitsarchitektur überdenken. Tun sie dies nicht, laufen sie Gefahr, den Fluss von Applikationen über Segmentgrenzen und Perimeter hinweg nicht mehr kontrollieren zu können. Das Unternehmen Palo Alto Networks™ gibt richtungsweisende Antworten und stellt sich mit seinen PAN-Appliances an die technologische Spitze.

Andreas Mertz

Der Autor ist Principal Consultant bei IT-CUBE SYSTEMS, einem auf IT-Security spezialisierten Systemintegrator. Das Unternehmen ist eines der ersten, die PAN-Systeme in komplexen Umgebungen erfolgreich implementiert haben.