It’s Time to Fix The Firewall

Die „Firewalls der nächsten Generation” von Palo Alto Networks erobern den angestammten Platz der Firewalls als „Eckpfeiler der Unternehmensnetzwerksicherheit” zurück.

Februar 2009

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA 94089
408-738-7700
www.paloaltonetworks.com

Inhalt

Zusammenfassung

Firewalls, die Ports und IP-Adressen überwachen, waren die letzten 15 Jahre State of the Art der IT-Sicherheitsstrategien von Unternehmen. IT-Anwendungen und Nutzerverhalten veränderten sich jedoch im Laufe der Zeit grundlegend und mit ihnen auch die Bedrohungsszenarien. Objektiv betrachtet ist mit herkömmlichen Firewalls kein umfassender Schutz der Unternehmensnetze mehr gewährleistet. Die Kernprobleme für die laufenden Anwendungen im Netz und zu wenig Kontrolle über Programme und Nutzer, versuchen die Firewall-Anbieter bisher zu lösen, indem sie zusätzliche Sicherheitsfunktionen aufsetzen – jedoch mit wenig Erfolg. Hinzu kommt, dass diese Maßnahmen, die die IT-Sicherheit in Unternehmen ergänzen sollen, umständlich und kostspielig sind.

Das Ergebnis: Die Wirksamkeit der Sicherheitsinfrastruktur nimmt ab, gleichzeitig steigen die Komplexität und die Kosten für deren Aufbau und Wartung. Diese Situation ist für Unternehmen auf Dauer nicht tragbar.

Palo Alto Networks entwickelt eine Produktfamilie von Firewalls der nächsten Generation, die den neuen Gefahrensituationen im Unternehmensnetzwerk gerecht wird. Die Firewalls fokussieren anstatt Ports und IP-Adressen Anwendungen, Nutzer und Inhalte, sie liefern damit Transparenz und Kontrolle im Unternehmensnetz. Der Ansatz für die Klassifizierung des Datenverkehrs dieser neuen Firewalls ist also anwendungszentriert und sie verfügen über innovative Erkennungstechnologien. Damit und auf Basis einer hochleistungsfähigen Architektur ist die Wirksamkeit von Unternehmens-Firewalls wieder gewährleistet, und es werden sogar deren Kernfunktionen noch erweitert – vor allem in den Bereichen Bedrohungsabwehr und Inhaltskontrolle. Mit den Firewalls der nächsten Generation von Palo Alto Networks können Unternehmen guten Gewissens zeitgemäße, innovative, webbasierte Applikationen einsetzen ohne die Risiken einzugehen, denen sie mit herkömmlichen Firewall-Technologien ausgesetzt wären. Die IT kann sich auf geschäftsrelevante Elemente, wie Anwendungen, Benutzer und Inhalte beim Einrichten und Durchsetzen von Richtlinien konzentrieren. Risiken werden umfassender und effektiver gehandhabt, die Kosten der IT-Sicherheit sinken.

Neue Anwendungen und Bedrohungen sind schwer fassbar

In den vergangenen Jahren haben sich Anwendungen und Nutzerverhalten verändert – und damit auch die Bedrohungsszenarien.

Personal Applications sind allgegenwärtig

Benutzerzentrierte Anwendungen wie Instant Messaging, Peer-to-Peer-Filesharing (P2P), Webmail sowie eine Unmenge von sozialen Netzwerken sind mittlerweile allgegenwärtig – auch in Unternehmensnetzwerken und auch wenn die Richtlinien eines Unternehmens den Einsatz dieser Programme untersagen. Skype, BitTorrent oder YouTube sind aber nicht nur äußerst populär, sondern auch so konzipiert, dass sie sich traditionellen Gegenmaßnahmen wie etwa der Erkennung durch herkömmliche Firewalls entziehen. Sie nehmen nicht die konventionellen Wege, sondern passen ihre Kommunikationsweise dynamisch an. Zu den häufigen „Umgehungsmethoden“ gehören:

- Port-Hopping, dabei werden Ports/Protokolle im Verlauf einer Sitzung nach dem Zufallsprinzip gewechselt.
- Die Nutzung nicht standardmäßiger Ports. Yahoo! Messenger nutzt beispielsweise TCP-Port 80 anstelle von TCP-Port 5050.
- Tunneling innerhalb häufig genutzter Dienste, wenn z. B. das P2P-Filesharing oder ein IM-Client wie Meebo über HTTP ausgeführt wird.
- Verbergen innerhalb einer SSL-verschlüsselten Verbindung.

Geschäftsanwendungen imitieren Personal Applications

Mehrere eng miteinander verknüpfte Entwicklungen machen die Sache kompliziert: Viele der oben erwähnten Anwendungen erweisen sich nicht nur für die persönliche, private Kommunikation als äußerst nützlich, sondern werden von Unternehmen weltweit routinemäßig auch für geschäftliche Zwecke verwendet. Die Absichten und auch die Resultate sind dabei durchaus positiv für das Unternehmen: Betriebsabläufe werden beschleunigt und erleichtert, eine schnelle und unkomplizierte Kommunikation und Zusammenarbeit ist gewährleistet, die Ausfallquote für Kunden, Partner und die eigenen Abteilungen werden minimiert.

Dabei entsteht jedoch eine Sicherheitsproblematik, denn moderne Geschäftsanwendungen sind häufig so konzipiert, dass sie sich dieselben „Umgehungstechniken“ zunutze machen, wie die Personal Applications. Der unbeabsichtigte und eindeutig negative Nebeneffekt ist dabei, dass dem Unternehmen der Überblick und die Kontrolle über die Netzwerkkommunikation und das Wissen, welche Anwendungen im Firmennetz laufen, immer mehr verloren gehen.

Ein dritter relevanter Faktor kommt hinzu: Unternehmensanwendungen arbeiten zunehmend webbasiert. Um die Zugriffsmöglichkeiten zu verbessern und den Verwaltungsaufwand und die Kosten zu senken, werden klassische Client-Server-Anwendungen auf Web-Technologien umgestellt. Alternativ werden Anwendungen komplett ersetzt durch gehostete,

webbasierte Dienste wie Salesforce, WebEx und Google Apps. Das Ergebnis: Rund zwei Drittel des gesamten Datenverkehrs im Unternehmen nutzen die Protokolle HTTP und HTTPS. An sich kein Problem, allerdings spitzt sich eine inhärente Schwäche traditioneller Sicherheitsinfrastrukturen dadurch weiter zu: Besonders ältere Firewalls können bei Anwendungen, die über HTTP kommunizieren, nicht unterscheiden, ob sie einem legalen Geschäftszweck dienen oder nicht.

Von der Motivation Profit und von Huckepack-Anwendungen

Die Bedrohungsszenarios haben sich erheblich verändert. Die Motivation der Verursacher ist eine andere geworden. Wollten sich die Missetäter früher „nur einen Namen machen“, wird jetzt in großem Umfang mit Hacking richtig Geld verdient. Nicht der Schaden, der angerichtet wird, zählt, sondern die Daten, die dort zu holen sind, oder die Botnets, die über Trojaner errichtet werden. Entsprechend ist das Ziel der Hacker, Abwehrsysteme auszutricksen. Und derzeit besteht eine beliebte Methode darin, sich über den Application-Layer „einzuschleichen“. „Huckepack auf der Anwendung“ können die Schadprogramme die Mehrzahl der unternehmenseigenen herkömmlichen Abwehrsysteme ungehindert durchlaufen, da diese lediglich für einen Schutz auf dem Netzwerk-Layer ausgelegt sind.

Die Hacker von heute widmen vor allem den beliebten und weit verbreiteten benutzerzentrierten Anwendungen (Social Applications) große Aufmerksamkeit. Deren „Umgehungsstrategien“ in und aus den Netzwerken lassen sich ideal dazu nutzen, Bedrohungen in Unternehmensnetzwerke einzuschleusen. Grund genug für das SANS Institute, inzwischen Instant Messaging- und Peer-to-Peer-Programme in seine Liste der SANS Top-20 Sicherheitsrisiken aufzunehmen.

Außer Kontrolle

Als Folge all dieser Veränderungen hat die IT die Kontrolle verloren. Und Unternehmen hatten bisher wenig Chancen, die Kontrolle zurück zu erlangen: Denn ihre herkömmliche Sicherheitsinfrastruktur kann zwischen guten erwünschten und schädlichen unerwünschten Anwendungen nicht effektiv unterscheiden. Entweder wird also weitergemacht wie bisher, um die Verfügbarkeit erwünschter Anwendungen sicherzustellen. Allerdings bleibt dabei alles ungeprüft, was mit modernen Anwendungen der nächsten Generation verbunden ist. Oder es wird versucht, schädliche und unerwünschte Sessions so gut wie möglich mit den verfügbaren Tools einzudämmen, die zur Hand sind. Dies hat allerdings nur wenig Aussicht auf Erfolg und führt oft dazu, dass das Nützliche zusammen mit dem Schädlichen verworfen wird.

Um die Sache wieder ins Lot zu bringen, braucht es Sicherheitstechnologie mit Intelligenz, die unterscheiden kann:

- Welcher Netzwerkdatenverkehr gehört zu Anwendungen, die einem legitimen Geschäftszweck dienen?
- Welcher Netzwerkdatenverkehr entspricht Anwendungen, die einem legitimen Geschäftszweck dienen können, aber in einem bestimmten Fall auch missbraucht werden können?

- Welcher Netzwerkdatenverkehr soll blockiert werden, obwohl er legitimen Geschäftsaktivitäten entspricht, weil er Malware oder andere Arten von Bedrohung enthält?

Firewalls mit Port-Kontrolle sind ineffektiv

Von der Unternehmensfirewall wird normalerweise eine detaillierte und genaue Zugriffskontrolle erwartet. Da die herkömmlichen Firewalls die Fähigkeit haben, den Kommunikationsverkehr zu steuern, werden sie seit jeher an strategischen Punkten positioniert, um Bereiche mit unterschiedlichen Vertrauensstufen abzugrenzen, wie z. B. am Internet-Gateway, an Verbindungsstellen zu Partnernetzwerken und, seit kurzem, an der logischen Vordertür des Rechenzentrums.

Den meisten Firewalls fehlt jedoch im wahrsten Sinne des Wortes der Durchblick. Dies liegt an ihrer Vorgehensweise: Sie schließen von der Portnummer auf den Dienst des Application-Layers, mit dem ein bestimmter Datenverkehrsstrom verbunden ist. Dabei stützen sie sich auf die überkommene Konvention, dass ein bestimmter Port immer einem bestimmten Dienst entspricht (z. B. TCP-Port 80 entspricht HTTP). Doch das ist längst überholt. Insofern können sie auch nicht erkennen, dass es sich um unterschiedliche Anwendungen handelt, sobald sie nur denselben Port nutzen.

Abbildung 1: Portblockierende Firewalls können Anwendungen weder sehen noch kontrollieren

Herkömmliche Port-basierte Firewalls sind damit im Grunde blind gegenüber Anwendungen einer neuen Generation. Gängige Umgehungstechniken wie Port-Hopping, Protokoll-

Tunneling oder die Verwendung von nicht standardmäßigen Ports berücksichtigen sie nicht. Ihnen fehlt damit die oben geforderte Transparenz und Intelligenz, die eine moderne Firewall mitbringen muss. Unternehmen, die sich weiterhin auf sie verlassen – sowie auf andere Gegenmaßnahmen, die an denselben Einschränkungen kranken –, nehmen in Kauf, dass die Nutzer in ihren Netzwerken schalten und walten können, wie es ihnen beliebt. Und das ist gefährlich.

Firewall-Nachbesserungen haben versagt

Unternehmen ergreifen meist zwei Maßnahmen, von denen sie sich versprechen, die Unzulänglichkeiten ihrer herkömmlichen Firewalls zu beheben. Leider erweisen sich beide als vollkommen nutzlos.

Deep Packet Inspection ist fehlerbehaftet

Die Einbindung von Deep Packet Inspection-Funktionen (DPI) soll die „Kurzsichtigkeit" traditioneller Firewall-Produkte korrigieren. Oberflächlich betrachtet mag das für den Anwendungslayer ein vernünftiger Ansatz sein. Allerdings wird nur teilweise mehr Sicherheit erreicht, da die zusätzliche Funktion lediglich auf Bestehendes „aufgesetzt" wird, der Unterbau bleibt weiterhin anfällig. Die Firewall, die nur Ports kontrolliert, wird nach wie vor für die anfängliche Klassifizierung des gesamten Datenverkehrs verwendet und kann Anwendungen nicht zuverlässig erkennen. Das hat folgende Auswirkungen:

- Nicht alles, was überprüft werden sollte, wird auch überprüft. Da die Firewall den Anwendungsdatenverkehr nicht akkurat klassifizieren kann, wird die Entscheidung, welche Sessions über das DPI-Modul geleitet werden sollen, zur Glückssache. Da die Firewall den Anwendungsdatenverkehr nicht akkurat klassifizieren kann, wird die Entscheidung, welche Sessions über das DPI-Modul geleitet werden sollen, zur Glückssache.
- Die Policy-Verwaltung wird extrem kompliziert. Die Regeln für die Behandlung einzelner Anwendungen werden im DPI-Teil des Produkts verschachtelt, der selbst Teil einer Zugriffssteuerung auf höher Ebene ist.
- Unzulängliche Leistung erzwingt Kompromisse. Die ineffiziente Nutzung von Systemressourcen und der CPU sowie speicherintensive Funktionalität auf dem Application-Layer belasten das System erheblich. Um dieser Situation Rechnung zu tragen, können Administratoren moderne Filterfunktionen nur selektiv einsetzen.

Firewall-Helfer lösen das Problem nicht und führen zu komplexen und teuren Systemen

In Erkenntnis der unbefriedigenden Situation versuchen Unternehmen, die Defizite ihrer Firewall durch den Einsatz verschiedener zusätzlicher Sicherheitslösungen zu kompensieren. Meist handelt es sich dabei um eigenständige Appliances (Boxen) für Intrusion Prevention, Webfiltering, Antivirus und anwendungsspezifische Lösungen wie eine dedizierte Plattform für Instant-Messaging-Sicherheit – um nur einige zu nennen. Leider ist das Ergebnis ähnlich enttäuschend wie beim DPI-Ansatz – ergänzt um so manche zusätzliche Komplikation.

Aber auch dieser Park von Zusatzgeräten überprüft nicht all das, was überprüft werden sollte. Denn entweder sehen auch sie nicht den gesamten Datenverkehr, oder sie stützen sich auf dieselben unzulänglichen port- und protokollbasierten Klassifikationsschemen, die bereits bei der alten Firewall versagt haben, oder sie decken nur eine begrenzte Anzahl von Anwendungen ab. Die komplizierte Policy-Verwaltung, die mit dem Einsatz dieser Geräte einhergeht, ist ein noch größeres Problem, da die Zugriffsregeln und Überprüfungsanforderungen auf mehrere Konsolen verteilt sind. Die Systemleistung stellt ebenfalls oft ein Problem dar, zumindest was eine relativ hohe Gesamtlatenz angeht.

Schlussendlich kommen die Kosten ins Spiel. Dem Netzwerk wird eine „Lösung“ nach der anderen hinzugefügt, die Geräteanzahl, der Komplexitätsgrad und die Gesamtkosten (TCO) nehmen immer weiter zu. Zu den Investitionskosten für die Produkte selbst und für die erforderliche Infrastruktur addieren sich laufende Betriebsausgaben wie Support- und Wartungsverträge, Lizenz- und Versorgungskosten (Energie, Kühlung, Stellraum), sowie eine Reihe weicher Kosten, die IT-Produktivität, Schulung und Lieferantenverwaltung betreffen. Das Ergebnis sind schwerfällige, ineffektive und kostspielige Systeme, die sich nicht lohnen.

It´s Time to fix the Firewall

Firewalls sehen grundsätzlich den gesamten Datenverkehr, da sie an kritischen Netzwerkknoten eingesetzt werden. Daher sind sie das ideale Mittel zur Durchsetzung einer Kontrolle. Die eine Problematik besteht darin, dass ältere Firewalls gegenüber Anwendungen und Bedrohungen der neuesten Generation blind sind. Eine weitere ist, dass sich alle Verbesserungsversuche lediglich darauf konzentriert haben, die Defizite zu beheben. Es stellt sich deshalb folgende Frage: Warum packt keiner das Problem an seiner Wurzel?

Warum ersetzt nicht eine einzige Lösung die Palette von Zusatzlösungen und erfüllt die wesentlichen funktionellen Anforderungen an eine wirklich wirksame, moderne Firewall, die Folgendes leistet:

- Identifikation von Anwendungen, unabhängig von Port, Protokollen, Umgehungsmethoden oder SSL-Verschlüsselung.
- Detaillierte Übersicht und Transparenz sowie Richtlinienkontrolle über Anwendungen einschließlich einzelner Funktionen.
- Exakte Identifizierung von Benutzern und anschließende Verwendung der Erkennungsinformationen für die Richtlinienkontrolle.
- Echtzeitschutz vor einer großen Anzahl von Bedrohungen, u. a. vor denen, die auf der Anwendungsebene operieren.
- Unterstützung des Multi-Gigabit in-line-Einsatzes mit vernachlässigbaren Performance-Beeinträchtigungen.

Vorstellung von Palo Alto Networks und der Firewall der nächsten Generation

Nir Zuk, Sicherheitsvisionär und Miterfinder der Stateful Inspection Technologie, erkannte die neuen Herausforderungen, die sich durch die neueste Generation von Anwendungen und Bedrohungen stellten, und gründete im Jahr 2005 das Unternehmen Palo Alto Networks. Mit seinem Management-Team, das aus erfahrenen Experten der Netzwerksicherheitsbranche besteht, und unterstützt von hochkarätigen Investoren, machte er sich daran, die Effektivität der Unternehmensfirewall wieder herzustellen und das Problem bei seiner Wurzel zu packen. Palo Alto Networks verfolgt einen anwendungszentrierten Ansatz bei der Datenverkehrsklassifizierung, um die vollständige Transparenz und Kontrolle aller existenten Arten von Anwendungen, die in Unternehmensnetzwerken ausgeführt werden, zu gewährleisten. Das Ergebnis dieser Arbeit ist die Produktfamilie der „Next Generation Firewalls“ von Palo Alto Networks. Sie erfüllt als einzige Firewall-Lösung weltweit alle funktionellen Anforderungen an eine moderne, zeitgemäße Sicherheitslösung.

Einzigartige Erkennungstechniken stellen Transparenz und Kontrolle wieder her

Drei Technologien sorgen in den Firewalls der nächsten Generation von Palo Alto Networks für hohe Transparenz und Kontrolle: App-ID, User-ID und Content-ID. Unternehmen können sich damit auf geschäftsrelevante Elemente konzentrieren, wie Regeln für Anwendungen, Benutzer und Inhalte.

App-ID – positive Identifikation von Anwendungen, unabhängig von Port, Protokoll, Umgehungsmethode oder SSL-Verschlüsselung

Die Technologie zur Datenverkehrsklassifizierung App-ID bildet das Kernstück der Firewall der nächsten Generation. Mithilfe vier verschiedener Techniken ist sie in der Lage, die genaue Identität von mehr als 750 Anwendungen im Netzwerk zu bestimmen, unabhängig von Port, Protokoll, SSL-Verschlüsselung oder Umgehungsmethoden. App-ID ist zum Patent angemeldet.

Erkennung und Entschlüsselung von Anwendungsprotokollen. In diesem ersten Schritt wird das Anwendungsprotokoll (z.B. HTTP) bestimmt und, bei Verwendung von SSL, der Datenverkehr entschlüsselt. Dann wird er weiter analysiert. Bei Bedarf findet eine Wiederverschlüsselung statt, nachdem alle Identifikationstechnologien zum Einsatz gekommen sind.

Decodierung des Anwendungsprotokolls. Diese Technik bestimmt, ob es sich bei dem anfänglich erkannten Anwendungsprotokoll um ein echtes Protokoll handelt oder ob es als Tunnel genutzt wird, in dem sich die tatsächliche Anwendung verbirgt (z. B. kann Yahoo! Instant Messenger in HTTP verpackt sein).

Anwendungssignaturen. Anhand von kontextbasierten Signaturen wird nach eindeutigen Eigenschaften und Transaktionsmerkmalen gesucht, um die Anwendung richtig und unabhängig vom verwendeten Port und Protokoll zu identifizieren. Dazu gehört auch die Erkennung bestimmter Funktionen innerhalb von Anwendungen, z. B. Dateiübertragungen innerhalb von IM-Sitzungen oder die Desktop-Freigabe innerhalb von Konferenzanwendungen.

Heuristik. Bei Datenverkehr, der sich nicht durch eine Signaturanalyse identifizieren lässt, werden zusätzliche heuristische oder verhaltensbezogene Prozesse angewendet. Dies ermöglicht die Identifizierung von Anwendungen wie Peer-to-Peer- oder VoIP-Tools, die eine proprietäre Verschlüsselung verwenden.

Die Erkennung ist nur ein Teil des Problems, deshalb ergänzt Palo Alto Networks die Komponente App-ID durch einen Anwendungsbrowser. Dieses leistungsstarke Recherchetool liefert Administratoren eine Fülle von Informationen zu über 750 Anwendungen, so dass sie fundierte Entscheidungen in Bezug auf deren Kontrolle treffen können. Die Anwendungen lassen sich nach Kategorie, Unterkategorie, zugrunde liegender Technologie und verschiedenen anderen Merkmalen anzeigen, z.B.: Dateiübertragungsmöglichkeiten, bekannte Schwachstellen, die Fähigkeit, eine Erkennung zu umgehen, die Neigung, Bandbreite zu verbrauchen, Malware zu übertragen oder anderweitig missbraucht zu werden.

Mit App-ID gewinnen IT-Abteilungen die Transparenz und die Informationen, die erforderlich sind, um Richtlinien zu entwickeln und durchzusetzen, anhand derer sich die Anwendungen in ihren Netzwerken wirksam kontrollieren lassen.

User-ID – Transparenz und Kontrolle nach IP-Adresse, Nutzer oder Gruppe

Auf jeder Firewall-Plattform von Palo Alto Networks werden mit Hilfe der User-ID-Technologie standardmäßig IP-Adressen mit bestimmten Benutzeridentitäten verknüpft. Das Ergebnis liefert eine hohe Transparenz und Kontrolle über die Netzwerkaktivität jedes Benutzers. Durch die zusätzliche Integration in Microsoft Active Directory (AD) unterstützt der User Identification Agent von Palo Alto Networks dieses Ziel auf zweierlei Weise: Zunächst verifiziert und wartet er die Benutzer-IP-Adressen-Beziehung. Dazu kombiniert er verschiedenen Techniken zur Login-Überwachung, Abfrage der Arbeitsplatzrechner oder von erzwungenen Anmeldeseiten (Captive Portal). Anschließend kommuniziert er mit dem AD-Domänencontroller, um die relevanten Benutzerinformationen, wie z. B. Rollen- und Gruppenzuweisungen, zu erhalten. Der Administrator verfügt damit über wichtige Details, die ihn bei seinen Aufgaben unterstützen:

- Mehr Transparenz in Bezug auf die Frage, wer genau für den gesamten Anwendungs-, Inhalts- und Bedrohungsdatenverkehr im Netzwerk verantwortlich ist
- Die Benutzeridentität dient als Variable bei der Entwicklung der Richtlinien für die Zugriffssteuerung

- Erleichterung der Problembehandlung/Vorfallsbearbeitung und Verwendung in Berichten

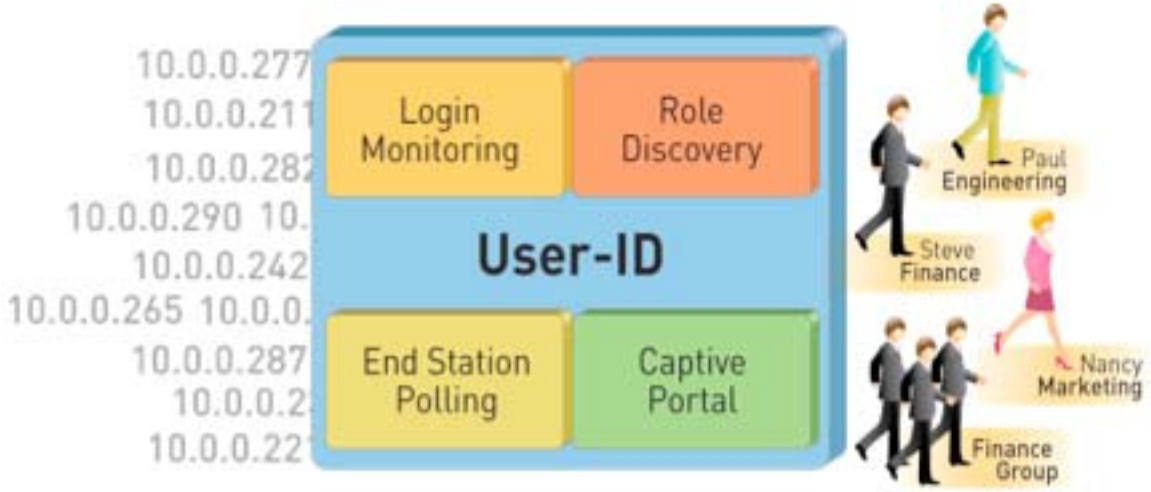

Abbildung 2: User-ID integriert Unternehmensverzeichnisse für benutzerbasierte Richtlinien und Berichterstellung

Mit der Komponente User-ID erhalten IT-Abteilungen einen weiteren leistungsfähigen Mechanismus, mit dessen Hilfe sich intelligent kontrollieren und steuern lässt, wer welche Anwendungen einsetzen darf. Beispielsweise kann die Nutzung eines Social Networks wie Facebook, das sonst aufgrund des hohen Risikos geblockt werden würde, für bestimmte Personen oder Gruppen aktiviert werden, die einen berechtigten Grund zu deren Nutzung haben, wie etwa die Personalabteilung.

Content-ID – leistungsfähige Inhaltsüberprüfung verhindert Bedrohungen, Zugang zu verbotenen Webinhalten und Verlust von vertraulichen Daten

Wie auch die beiden anderen Komponenten erweitert Content-ID die Firewalls von Palo Alto Networks um Funktionen, die bis dahin noch nie in einer Unternehmens-Firewall zum Einsatz gekommen sind. In diesem Fall handelt es sich um den Echtzeitschutz vor Sicherheitsrisiken in zulässigem Datenverkehr, die genaue Kontrolle über die Aktivitäten der User im Internet sowie ein Datei- und Daten-Filtering.

Abbildung 3: Content-ID vereinheitlicht die Inhaltsüberprüfung nach Bedrohungen, vertraulichen Daten und für URL-Filterung

Schutz vor Sicherheitsrisiken. Content-ID nutzt verschiedene, neuartige Funktionen, die das Eindringen von Spyware, Viren über Sicherheitslücken ins Netzwerk verhindern. Der Schutz funktioniert unabhängig davon, von welchem Typ die Daten sind oder von welcher Applikation sie stammen, die als Transportmittel dient.

- **Anwendungsdecoder:** Content-ID nutzt diese App-ID-Komponente, um Datenströme vorzubereiten, die dann auf bestimmte Bedrohungsmerkmale überprüft werden.
- **Stream-basierte Überprüfung auf Viren und Spyware**: **:** Im Gegensatz zu herkömmlichen Systemen beginnt die Überprüfung auf Gefahren bereits, wenn die ersten Pakete einer Datei eintreffen – nicht erst, wenn die komplette Datei in den Speicher geladen ist. Dies erhöht die Geschwindigkeit und verringert die Latenzzeit.
- **Einheitliches Format von Bedrohungssignaturen:** Durch das einheitliche Format sind keine separaten Überprüfungsmodule für jeden Bedrohungstyp nötig, was sich wiederum positiv auf die Verarbeitungsgeschwindigkeit auswirkt. Viren, Spyware und Exploits für Sicherheitslücken können in einem einzigen Durchlauf erkannt werden.
- **Schutz vor Angriffen auf Sicherheitslücken:** Neben robusten Routinen für die Vereinheitlichung und Defragmentierung des Datenverkehrs kommen Mechanismen zum Einsatz, die Abweichungen von den gängigen Protokollen und Verhalten erkennen, sowie heuristische Erkennungsmechanismen. Zusammen bieten sie einen umfassenden Schutz vor den verschiedensten bekannten und unbekannten Bedrohungen.

URL-Filterung. Eine integrierte URL-Datenbank erlaubt den Administratoren, die Internet-Aktivitäten von Mitarbeitern und Gastbenutzern zu überwachen und zu steuern. In Verbindung mit der Komponente User-ID können die Richtlinien für die Internetnutzung für jeden Benutzer individuell festgelegt werden. So lässt sich das Unternehmen vor Risiken schützen, die im Zusammenhang mit der Einhaltung von gesetzlichen Bestimmungen stehen, und auch vor solchen, die die Produktivität gefährden.

Datei- und Datenfilterung. Dank der leistungsfähigen Anwendungsfilter von App-ID lassen sich wirkungsvolle Regelwerke aufsetzen, die das Risiko einer nicht autorisierten Datenübertragung minimieren. So können beispielsweise Dateien abhängig von ihrem Typ blockiert werden – also nicht einfach auf Grundlage ihrer Dateierweiterung – oder die übertragenen Muster vertraulicher Daten wie Kreditkarten- oder Sozialversicherungsnummern werden kontrolliert. Diese Fähigkeiten ergänzen die Granularität von App-ID und bei vielen Anwendungen besteht dadurch die Möglichkeit, die Dateiübertragung auch in einzelnen Anwendungen zu kontrollieren.

Die Fähigkeiten von Content-ID versetzen IT-Abteilungen in die Lage, bekannte und unbekannte Bedrohungen zu stoppen, eine unzulässige, weil gefährdende Nutzung des Internets zu reduzieren und Datenverlust zu verhindern. Das Unternehmen muss dafür nicht in zusätzliche Produkte investieren, mit dem bekannten Kosten- und Ressourcen-Aufwand.

Sicherheit ohne Kompromisse durch leistungsfähige SP3-Architektur

Auch die größte Palette an Anwendungsfiltern, Inhaltsfiltern und Kontrollsystemen bringt wenig, wenn Administratoren sie nicht in vollem Umfang einsetzen können, weil Probleme mit der Systemleistung entstehen. Es geht dabei weniger darum, dass diese Funktionen von sich aus ressourcenintensiv sind, sondern um die enormen Datenvolumen, mit denen die heutige Sicherheitsinfrastruktur konfrontiert ist. Ganz zu schweigen von der Latenzempfindlichkeit vieler moderner Anwendungen.

Angesichts dieser Herausforderungen hat sich Palo Alto Networks von Anfang an das Ziel gesetzt, eine extrem leistungsfähige Lösung zu entwickeln. Jede einzelne Funktion wurde optimiert, um eine größtmögliche Effizienz zu erreichen. Ergebnis dieser Bemühungen sind beispielsweise die Stream-basierte Überprüfung und die Verwendung eines einheitlichen Formats für Bedrohungssignaturen. Ein bemerkenswerter Fortschritt auf der System-/Plattformebene in der Next Generation Firewall ist die Single-Pass-Parallel-Processing-Architektur (SP3), mit einer Single-Pass-Software (packet flow) und einer funktionsspezifischen Parallelverarbeitung.

Bei herkömmlichen Sicherheitslösungen, insbesondere bei jenen mit aufgesetzten Funktionen, wird jede High-Level-Sicherheitsfunktion unabhängig ausgeführt. Dieser „Multi-Pass-Ansatz“ erfordert die mehrmalige Wiederholung der Routinen für Paketverarbeitung und für die Reassemblierung von Datenströmen einer niedrigeren Ebene. Systemressourcen werden also ineffizient genutzt und es entstehen relativ große Latenzzeiten. Die Firewall der nächsten Generation von Palo Alto Networks arbeitet dagegen mit einem „Single-Pass-Ansatz“. Ihr strukturiertes und lineares Design vermeidet die wiederholte Verarbeitung von Paketen und Datenströmen und senkt damit die Belastung der Systemhardware und Latenzzeiten deutlich minimiert.

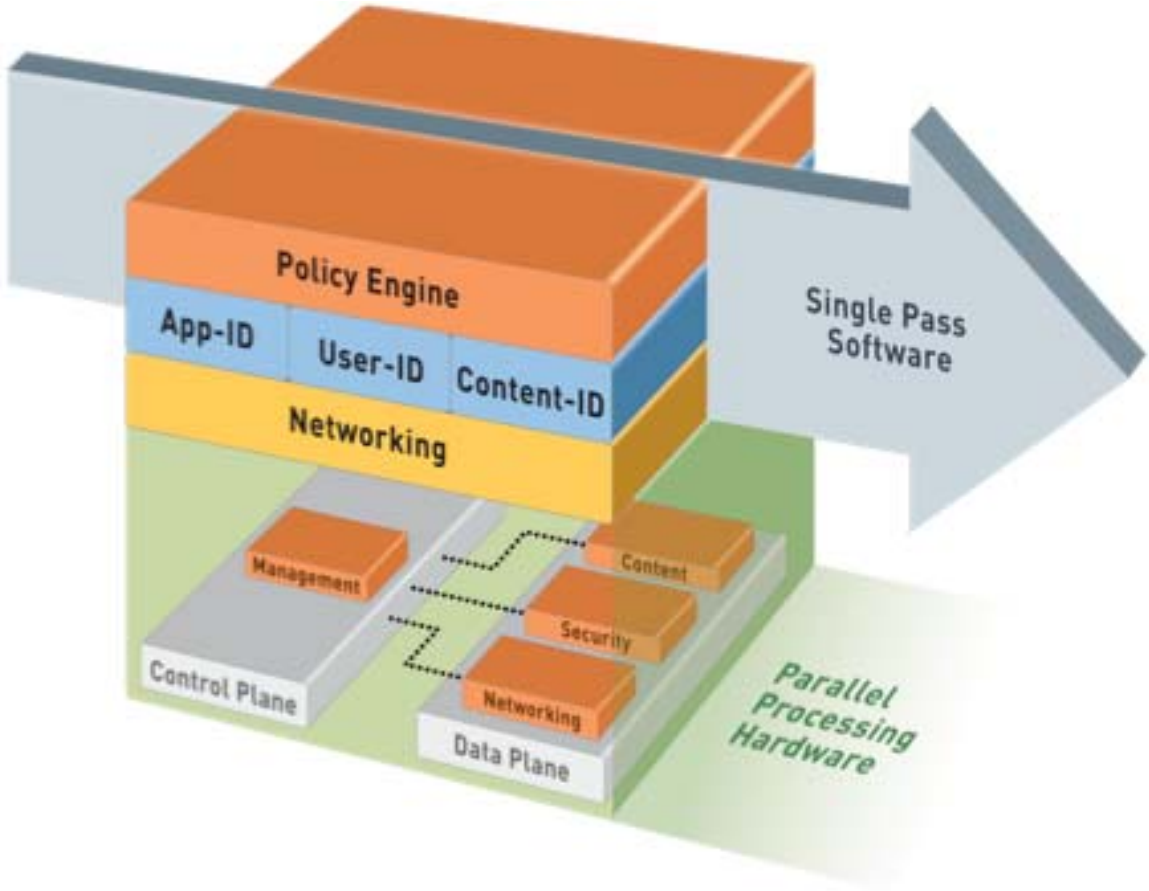

Abbildung 4: Single-Pass-Parallel-Processing-Architektur verbindet Software und Hardware von Unternehmen

Ein weiterer und gewichtiger Vorteil der SP3-Architektur von Palo Alto Networks: Sie ermöglicht eine funktionsspezifische Verarbeitung. Jede Firewall-Appliance verfügt über eine Platine für Managementfunktionen mit dedizierten CPUs, Speicher und Datenträger. Alle anderen Prozesse werden auf einer separaten Steckkarte ausgeführt. Dazu gehören:

- ein Netzwerkprozessor für die Paketverarbeitung und für Funktionen auf Netzwerk-Layer

- ein Multicore-Security-Prozessor mit Hardwarebeschleunigung für Standardfunktionen
- ein Hardwaremodul für die Inhaltsüberprüfung.

Die Firewalls der nächsten Generation von Palo Alto Networks wurden von Anfang an als Hochleistungslösung ausgelegt. Damit sind sie in der Lage, das gesamte Leistungsspektrum der von App-ID, User-ID und Content-ID zu liefern, ohne Kompromisse bei der Geschwindigkeit eingehen zu müssen. Eine sehr geringe Latenzzeit ist selbst bei voller Ausnutzung der Bandbreite garantiert.

Enterprise-Qualität durch zusätzliche Funktionen

Palo Alto Networks ist sich bewusst: Neben der Aufgabe, die Unzulänglichkeiten traditioneller Firewalls zu überwinden, muss die Next Generation Firewall auch praktische Problemen der Unternehmen berücksichtigen. Dazu gehören die Bereitstellung der Daten und ein reibungslos laufender Betrieb. Wichtige Überlegungen betreffen die Kompatibilität mit der bestehenden Infrastruktur, die Flexibilität bezüglich verschiedener Anwendungsfälle, hohe Zuverlässigkeit, Einfachheit und Benutzerfreundlichkeit. Deshalb wurde die Lösung mit den folgenden zusätzlichen Leistungsmerkmalen ausgestattet:

- Mit einem stabilen Netzwerkfundament, einschließlich Unterstützung von L2/L3-Switching, dynamischem Routing (OSPF, RIPv2), 802.1Q VLANs und gebündelten Ports,
- mit flexiblen Aufstellungsmöglichkeiten einschließlich eines out-of-band „Nur-Beobachten“-Modus, eines transparenten in-line-Betriebs und einer vollständig aktiven in-line-Firewall-Ersatz-Konfiguration,
- mit aktiv/passiv Hochverfügbarkeit mit voller Konfigurations- und Sitzungssynchronisierung,
- mit einem intuitiven und flexiblen Management einschließlich Kommandozeilenschnittstelle, Weboberfläche und zentralisierter Konsole mit einheitlichem Look and Feel, Unterstützung von Syslog und SNMP sowie umfangreichen Protokoll- und Berichtfunktionen.

Mit einer umfassenden Palette an Netzwerk-, Integrations- und Systemverwaltungsfunktionen stellt die Firewall der nächsten Generation von Palo Alto Networks sicher, dass die IT-Organisation genau das bekommt, was sie benötigt: eine zuverlässige Sicherheitslösung für ihr Unternehmen.

Der neue Eckpfeiler für Unternehmenssicherheit

Die Firewalls der nächsten Generation von Palo Alto Networks verstehen sich als wegweisende Sicherheitslösung für Unternehmen, die spürbare Vorteile bringt und mit denen CIOs für die Herausforderungen moderner Gefahrenszenarios gerüstet sind. Die Firewalls

- ermöglichen benutzerbasierte, portübergreifende Transparenz und Kontrolle für alle Anwendungen,
- stoppen Malware und Exploits für Sicherheitslücken in Anwendungen in Echtzeit,
- verringern die Komplexität der Sicherheitsinfrastruktur und ihrer Verwaltung,
- stellen eine Hochgeschwindigkeitslösung bereit, die moderne Anwendungen schützt, ohne ihre Leistung zu beeinträchtigen,
- verhindern Datenverlust,
- vereinfachen die PCI-Compliance.

Aus der Geschäftsperspektive bringt die Firewall der nächsten Generation von Palo Alto Networks Unternehmen folgende Vorteile:

- Besseres und sorgfältigeres Management von Risiken und Erreichen von Konformität durch nie da gewesene Transparenz, Informationen und Kontrolle über den Datenverkehr im Firmennetz.
- Förderung des Wachstums, indem moderne Anwendungen und aktuelle Technologien ohne Risiko sicher genutzt werden können.
- Senkung von Kosten, indem der Gerätepark konsolidiert wird, die Infrastruktur vereinfacht und der Betrieb effizienter wird.

Palo Alto Networks bietet mit seinen Next Generation Firewalls heutigen Unternehmen genau das, was sie benötigen, um die Kontrolle über ihre Netzwerke zurück zu gewinnen und alle Kompromisse in Sachen Informationssicherheit zu beenden. Sie bieten eine völlige Transparenz des Netzwerks und Kontrolle über Anwendungen und Nutzer und dadurch zuverlässigen Schutz vor drohenden Gefahren. Damit ist die Next Generation Firewall von Palo Alto Networks auf dem besten Weg, der Firewall ihren angestammten Platz als sicherer Eckpfeiler der Unternehmenssicherheit wieder zurückzugeben.