Übersicht über die Palo Alto Networks-Firewalls der nächsten Generation

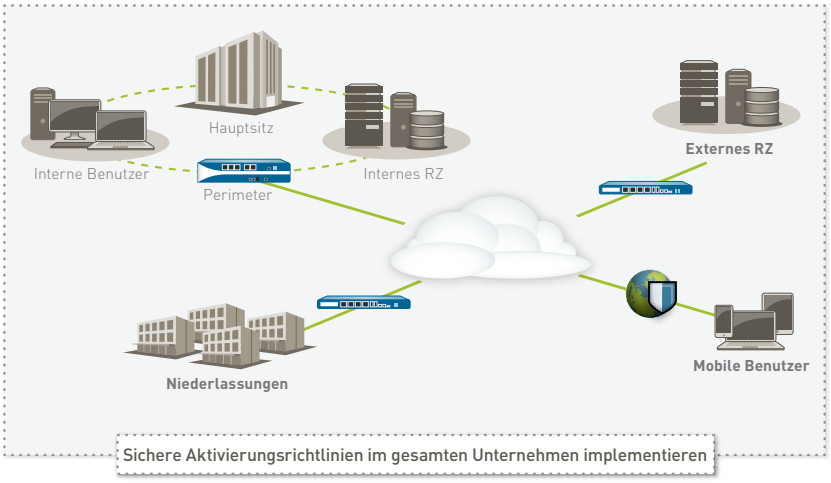
Wesentliche Änderungen auf dem Gebiet der Anwendungen und Bedrohungen, des Benutzerverhaltens und der Netzwerkinfrastruktur machen die Sicherheit, die traditionelle Port-basierte Firewalls früher geboten haben, mittlerweile unzureichend. Ihre Benutzer können unter Verwendung einer Reihe von Gerätetypen auf alle Arten von Anwendungen zugreifen, was oft für die Erledigung ihrer Arbeit erforderlich ist. Die Erweiterung der Rechenzentren, sowie Virtualisierung, Mobilität und Cloud-basierte Initiativen geben heute Anlass, die Methoden zur Aktivierung der Anwendungen bei gleichzeitigem Schutz Ihres Netzwerks zu überdenken.

Traditionelle Systeme bieten die Möglichkeit, sämtlichen Anwendungsverkehr über eine stetig wachsende Liste an Technologien, die zusätzlich zu den Firewalls eingesetzt werden, zu sperren, wodurch Ihr laufender Betrieb beeinträchtigt werden kann. Die andere Möglichkeit ist, alle Anwendungen zuzulassen, was aufgrund erhöhter Geschäfts- und Sicherheitsrisiken ebenfalls unzumutbar ist. Die Schwierigkeit besteht darin, dass Ihre traditionelle, Port-basierte Firewall selbst mit zusätzlicher Anwendungsblockierung keine Alternative zu diesen Ansätzen bietet. Um nicht alles erlauben oder alles verbieten zu müssen, müssen Sie eine sichere Aktivierung der Anwendungen mithilfe geschäftsrelevanter Elemente ermöglichen. Zu den wesentlichen Sicherheitsrichtlinien für eine Firewall gehört eine Anwendungsidentität, also wer die Anwendung nutzt und welche Art von Inhalt bereitgestellt wird.

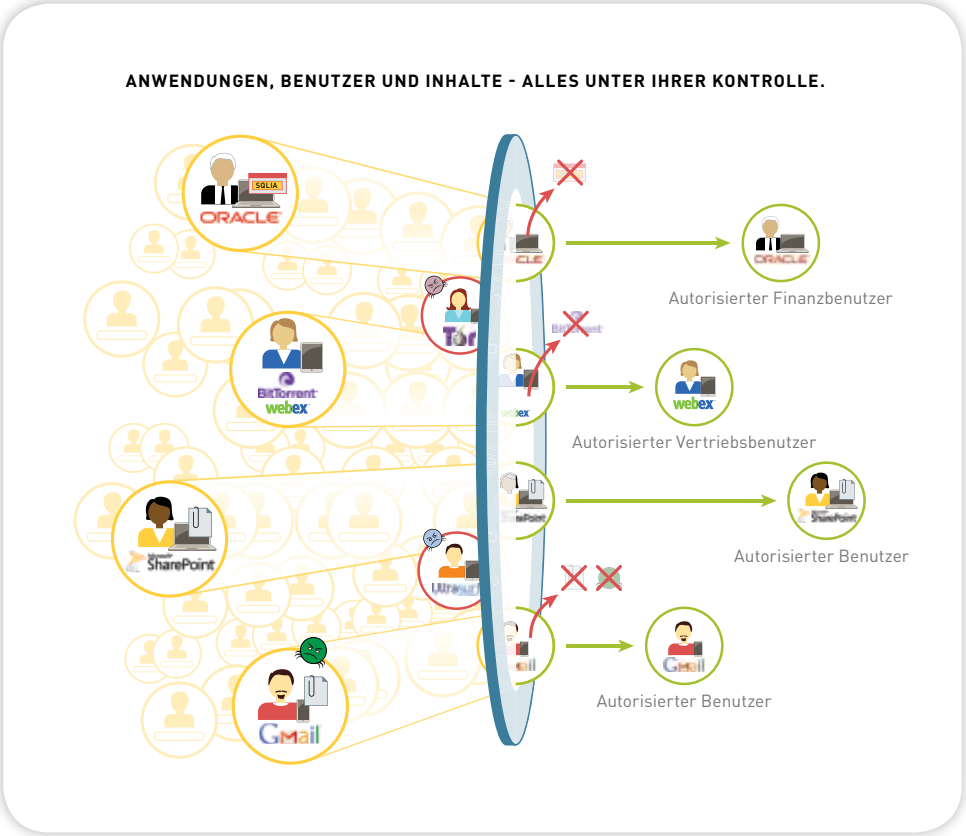
Wesentliche Anforderungen für eine sichere Aktivierung:

- **Identifikation von Anwendungen, nicht von Ports.** Klassifizieren des Verkehrs, sobald er die Firewall erreicht, um die Anwendungsidentität unabhängig von Protokoll, Verschlüsselung oder Umgehungsmethoden zu identifizieren. Diese Identität wird dann als Grundlage für alle Sicherheitsrichtlinien verwendet.
- **Verknüpfen der Nutzung der Anwendung mit der Benutzeridentität und nicht der IP-Adresse, unabhängig von Standort oder Gerät.** Implementieren von Benutzer- und Gruppeninformationen aus Unternehmensverzeichnissen und anderen Benutzerdatenbanken, um konsistente Aktivierungsrichtlinien für alle Benutzer unabhängig von Standort oder Gerät bereitzustellen.
- **Schutz vor sämtlichen bekannten und unbekannten Bedrohungen.** Verhindern von böswilligen URLs, dem Ausnutzen bekannter Schwachstellen und dem Eindringen von Malware und Spyware in das Netzwerk, während der Datenverkehr gleichzeitig danach durchsucht wird. Außerdem soll automatisch Schutz vor hochspezialisierter und bisher unbekannter Malware geboten werden.
- **Vereinfachte Richtlinienverwaltung.** Sichere Anwendungsaktivierung und geringerer Verwaltungsaufwand durch ein benutzerfreundliches grafisches Frontend, einen einheitlichen Richtlinien-Editor sowie Vorlagen und Gerätegruppen.

Mithilfe von Richtlinien zur sicheren Aktivierung von Anwendungen können Sie Ihre Sicherheit unabhängig vom Standort der Bereitstellung verbessern. Der Umfang der Bedrohungen lässt sich durch die Blockierung einer Reihe von unerwünschten Anwendungen und durch die Überprüfung der zulässigen Anwendungen auf Bedrohungen, ob bekannt oder nicht, reduzieren. In traditionellen oder virtuellen Rechenzentren sorgt die Anwendungsaktivierung dafür, dass nur Anwendungen des Rechenzentrums von autorisierten Benutzern verwendet werden. So lässt sich der Inhalt vor Bedrohungen schützen und die Sicherheitsanforderungen, die durch die Dynamik der virtuellen Infrastruktur entstehen, können erfüllt werden. Die Niederlassungen Ihres Unternehmens und mobile oder entfernte Benutzer können durch die gleichen Aktivierungsrichtlinien geschützt werden, die in Ihrem Hauptsitz implementiert sind, wodurch eine einheitliche Umsetzung der Richtlinien gewährleistet wird.



paloalto NETWORKS
the network security company™



Stärkung des Betriebs durch Anwendungsaktivierung

Mithilfe der sicheren Anwendungsaktivierung durch Palo Alto Networks-Firewalls der nächsten Generation können Sie Ihre Geschäfts- und Sicherheitsrisiken, die durch die wachsende Anzahl an Anwendungen in Ihrem Netzwerk entstehen, bekämpfen. Durch die Aktivierung von Anwendungen für Benutzer oder Benutzergruppen, ob lokal, mobil oder entfernt, und den Schutz des Verkehrs vor bekannten und unbekannten Bedrohungen können Sie Ihre Sicherheit verbessern und Ihren Geschäftserfolg gleichzeitig steigern.

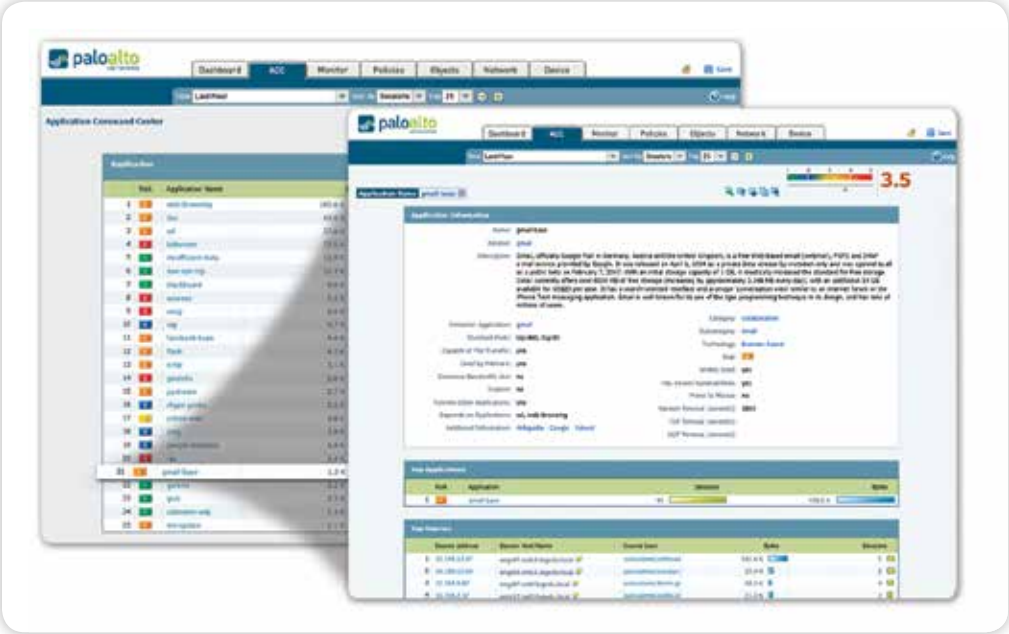
- **Klassifizierung aller Anwendungen auf allen Ports und zu jedem Zeitpunkt.** Eine exakte Klassifizierung des Datenverkehrs bildet das Kernstück jeder Firewall der nächsten Generation. Das Ergebnis wird zur Grundlage der Sicherheitsrichtlinie. Heute sind Applikationen in der Lage, eine herkömmliche Port-basierte Firewall ganz einfach zu umgehen: durch 'Port-Hopping' mit SSL und SSH, Tunneln über Port 80 oder die Nutzung nicht standardisierter Ports. App-ID zielt auf die Transparenzbeschränkungen bei der Verkehrsklassifizierung, unter der herkömmliche Firewalls gelitten haben. Dazu werden mehrere Klassifizierungsmechanismen auf den Verkehrsstrom angewendet, sobald die Firewall diesen entdeckt, um die genaue Identität von Anwendungen im Netzwerk zu erkennen, unabhängig von Port, Verschlüsselung (SSL oder SSH) oder Umgehungsmethoden. Das Wissen, welche Anwendungen, und nicht nur welcher Port und welches Protokoll, in Ihrem Netzwerk verwendet werden, wird zur Grundlage aller Entscheidungen zu den Sicherheitsrichtlinien. Nicht identifizierte Anwendungen (in der Regel nur ein kleiner Prozentsatz des Verkehrs, jedoch mit einem hohen Risiko behaftet), werden automatisch für die systematische Verwaltung kategorisiert. Diese kann eine Richtlinienkontrolle und -überprüfung, forensische Untersuchungen der Bedrohung, die Erstellung einer benutzerdefinierten App-ID oder eine Paketerfassung für die App-ID-Generierung durch Palo Alto Networks umfassen.

- **Integrieren von Benutzern und Geräten, nicht nur IP-Adressen, in die Richtlinien.** Die Erstellung und Verwaltung von Sicherheitsrichtlinien basierend auf der Anwendung und der Identität des Benutzers, unabhängig von Gerät oder Standort, ist eine effektivere Möglichkeit, Ihr Netzwerk zu schützen, als sich nur auf Port und IP-Adresse zu stützen. Durch die Integration in eine Vielzahl von internen Benutzer-Repositorys lässt sich die Identität der Benutzer, die über Microsoft Windows, Mac OS X, Linux, Android oder iOS auf die Anwendung zugreifen, ermitteln. Reisende oder entfernt arbeitende Benutzer werden nahtlos durch die gleichen, durchgängig geltenden Richtlinien geschützt, die auch im lokalen bzw. im Unternehmensnetzwerk eingesetzt werden. Dank der Kombination aus Transparenz und Kontrolle der Aktivität eines Benutzers in Bezug auf eine Anwendung ist die sichere Aktivierung von Oracle, BitTorrent, Google Mail oder einer beliebigen anderen Anwendung in Ihrem Netzwerk möglich, egal von wo oder wie der Benutzer darauf zugreift.

- **Verhindern sämtlicher bekannten und unbekannten Bedrohungen.** Um ein modernes Netzwerk schützen zu können, müssen verschiedene bekannte Schwachstellen, Malware und Spyware sowie völlig unbekannte und spezialisierte Bedrohungen in Betracht gezogen werden. Zunächst wird die Angriffsfläche im Netzwerk verringert, indem bestimmte Anwendungen zugelassen und andere abgelehnt werden. Dies erfolgt entweder bedingungslos über eine „Alles-andere-ablehnen"-Strategie oder über explizite Richtlinien. Anschließend kann ein koordinierter Bedrohungsschutz auf den zulässigen Verkehr angewendet werden, wobei bekannte Malware-Sites, Ausnutzungen von Schwachstellen, Viren, Spyware und böswillige DNS-Anfragen blockiert werden. Angepasste oder anderweitig unbekannte Malware wird durch Ausführen der unbekannten Dateien aktiv analysiert und identifiziert. Außerdem werden mehr als 100 schädliche Funktionsweisen in einer virtualisierten Umgebung direkt überwacht. Wenn neue Malware entdeckt wird, wird automatisch eine Signatur für die infizierte Datei und den zugehörigen Malware-Verkehr erstellt und an Sie übermittelt. Bei den Analysen zum Schutz vor Bedrohungen wird der vollständige Anwendungs- und Protokollkontext verwendet, um sicherzustellen, dass die Bedrohungen stets erfasst werden, selbst wenn sie versuchen, der Sicherheitsanalyse in Tunneln, komprimierten Dateien oder auf nicht standardmäßigen Ports zu entgehen.

Flexibilität bei der Bereitstellung und Verwaltung

Die Funktion zur sicheren Aktivierung von Anwendungen ist entweder über eine spezielle Hardware-Plattform oder in einem virtualisierten Formfaktor verfügbar. Wenn Sie mehrere Palo Alto Networks-Firewalls als Hardware oder virtualisierten Formfaktor implementiert haben, empfehlen wir Ihnen die Nutzung von Panorama, einer optionalen Lösung zur zentralen Verwaltung, mit der Sie Einblick in Datenmuster erhalten, Richtlinien umsetzen, Berichte erstellen und Inhaltsaktualisierungen von einem zentralen Standort aus bereitstellen können.



Anwendungstransparenz: Die Firewall zeigt die Aktivitäten im Zusammenhang mit Anwendungen in einem klaren und leicht zu interpretierenden Format an. Fügen Sie Filter hinzu und entfernen Sie diese wieder, um weitere Informationen über die Anwendung, ihre Funktionen und ihre Benutzer zu erhalten.

Sichere Anwendungsaktivierung: ein umfassender Ansatz

Eine sichere Aktivierung erfordert einen umfassenden Ansatz zur Sicherung Ihres Netzwerks bei gleichzeitiger Steigerung Ihres Geschäftserfolgs. Voraussetzung dafür ist eine detaillierte Kenntnis der Anwendungen in Ihrem Netzwerk, des Benutzers unabhängig von Plattform oder Standort und der ggf. von der Anwendung bereitgestellten Inhalte. Durch eine vollständigere Kenntnis Ihrer Netzwerkaktivitäten können Sie sinnvollere, für Ihr Unternehmen relevante Sicherheitsrichtlinien basierend auf Anwendung, Benutzer und Inhalt erstellen. Dabei machen Standort des Benutzers, die Plattform und der Ort, an dem die Richtlinie implementiert ist – Perimeter, traditionelles oder virtualisiertes Rechenzentrum, Niederlassung oder Remote-Benutzer – kaum einen Unterschied bei der Erstellung der Richtlinie. Sie können nun jede Anwendung, jeden Benutzer und jeden Inhalt sicher aktivieren.

Strengere Sicherheitsrichtlinien durch umfassendes Wissen

Bewährte Vorgehensweisen im Bereich der Sicherheit haben gezeigt, dass eine umfassende Kenntnis der Aktivitäten in Ihrem Netzwerk bei der Implementierung von strengeren Sicherheitsrichtlinien von Vorteil ist. Wenn Administratoren wissen, welche Anwendungen in Ihrem Netzwerk verwendet werden und nicht nur den Port-basierten Verkehr verfolgen können, können sie genau die Anwendungen zulassen, die Ihr Unternehmen benötigt, und gleichzeitig ungewünschte Anwendungen blockieren. Die Kenntnis des Benutzers und nicht nur der IP-Adresse ist ein weiteres Sicherheitskriterium, durch das Sie bei der Zuweisung der Richtlinien gezielter vorgehen können.

- Mithilfe von leistungsstarken grafischen Virtualisierungs-Tools erhalten Ihre Administratoren ein vollständigeres Bild der Anwendungsaktivität und des potenziellen Sicherheitsrisikos und können so fundiertere Richtlinienentscheidungen treffen. Die Anwendungen werden ständig klassifiziert und sobald sich ihr Zustand ändert, werden die grafischen Zusammenfassungen, die die Informationen auf einer benutzerfreundlichen, webbasierten Oberfläche anzeigen, automatisch aktualisiert.
- Neue oder unbekannte Anwendungen können mit einem Klick schnell untersucht werden. Auf diese Weise werden eine Beschreibung der Anwendung, ihre wichtigsten Funktionen, ihre Verhaltenseigenschaften und ihre Benutzer angezeigt.
- Die zusätzliche Transparenz im Hinblick auf URL-Kategorien, Bedrohungen und Datenmuster bietet ein vollständiges und abgerundetes Bild der Netzwerkaktivität.
- Unbekannte Anwendungen (in der Regel ein kleiner Prozentsatz in jedem Netzwerk, jedoch mit einem hohen Risiko behaftet), werden für eine Analyse kategorisiert, bei der bestimmt wird, ob es sich um interne Anwendungen, noch nicht identifizierte kommerzielle Anwendungen oder Bedrohungen handelt.

Anwendungen aktivieren und gleichzeitig das Risiko senken

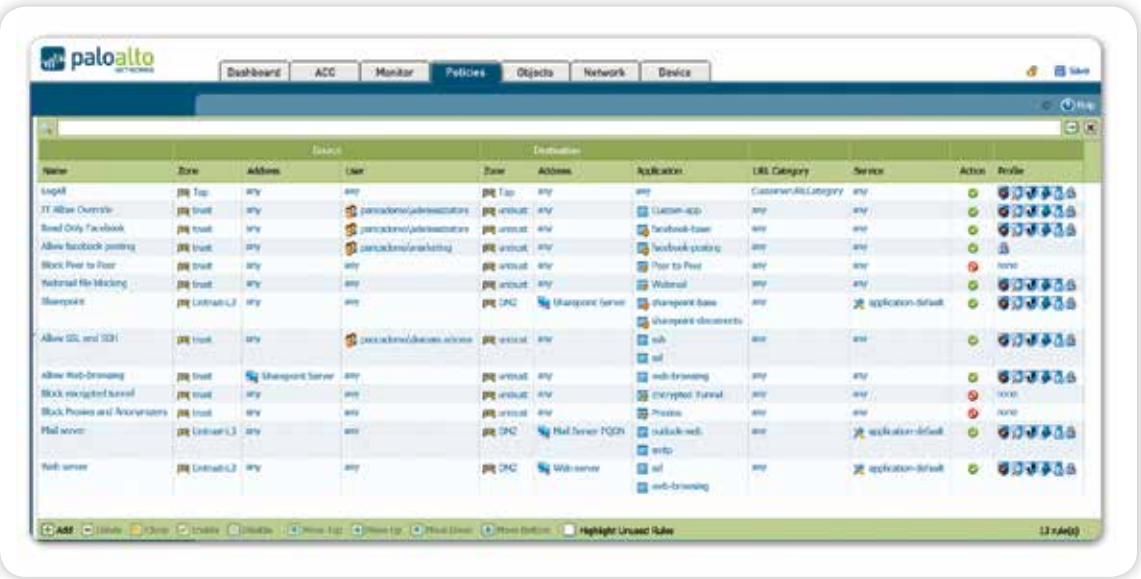
Bei der sicheren Aktivierung von Anwendungen werden Entscheidungskriterien bei der Erstellung der Richtlinien verwendet, die die Anwendung/Anwendungsfunktion, Benutzer und Gruppen sowie den Inhalt umfassen. Dadurch soll ein Mittelweg zwischen der Ablehnung aller Anwendungen, was den Geschäftsbetrieb einschränken würde, und dem hohen Risiko, das durch die Zulassung alle Anwendungen entstehen würde, gefunden werden.

Die Aktivierungsrichtlinien konzentrieren sich an der Grenze, also bei den Niederlassungen, bei mobilen und entfernten Benutzern, auf die Identifizierung des gesamten Verkehrs. Dieser wird dann basierend auf der Benutzeridentität selektiv zugelassen und anschließend auf Bedrohungen überprüft. Beispiele für Richtlinien sind unter anderem:

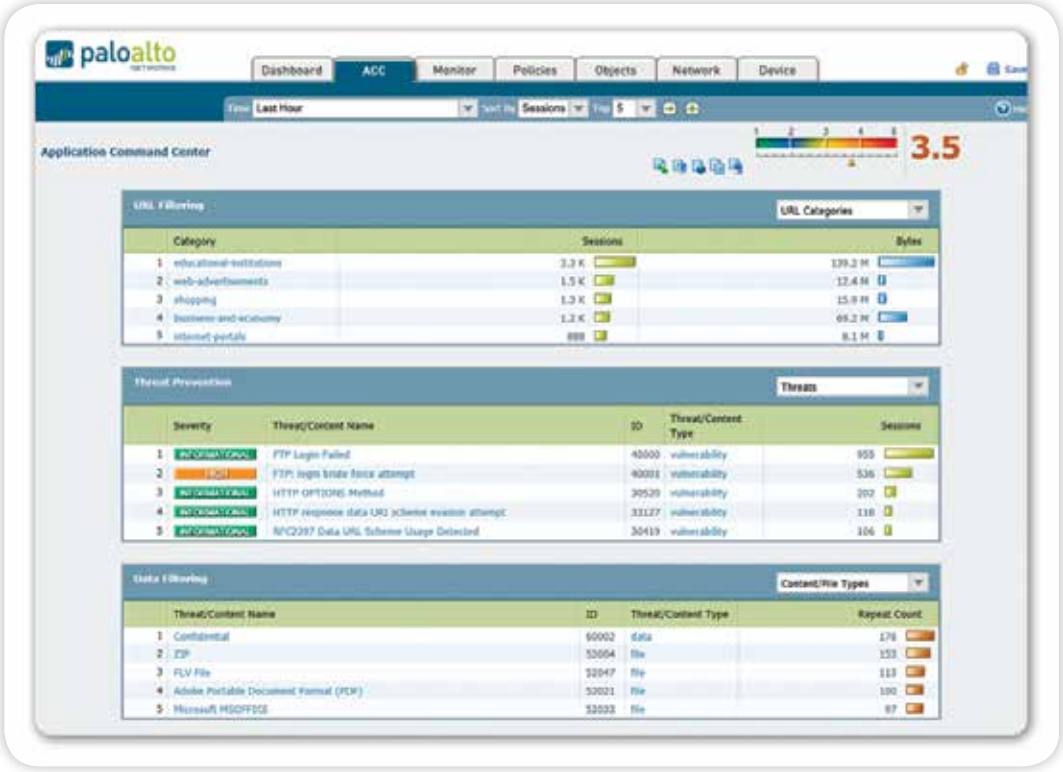
- Beschränkung der Nutzung von Webmail und Instant Messaging auf wenige ausgewählte Varianten, Entschlüsselung derjenigen, die SSL verwenden, Überprüfung des Verkehrs auf Schwachstellen und Hochladen von unbekannten Dateien in WildFire™ zu Analyse- und Signaturerstellungszwecken
- Zulassen von gestreamten Medienanwendungen und Websites, jedoch nur unter Anwendung von QoS und Malware-Schutz, um die Auswirkungen auf VoIP-Anwendungen zu beschränken und Ihr Netzwerk zu schützen
- Kontrolle von Facebook, indem Ihren Benutzern das „Durchsuchen“ gestattet ist, jedoch alle Facebook-Games und sozialen Plug-ins blockiert werden. Das Posten von Beiträgen wird nur zu Marketingzwecken gestattet. Analysieren des Facebook-Verkehrs auf Malware und die Ausnutzung von Schwachstellen
- Kontrolle des Surfens im Internet, indem geschäftlich genutzte Websites zugelassen und überprüft werden, während der Zugriff auf offensichtlich für private Zwecke genutzte Websites blockiert wird, und „Coaching“ des Zugriffs auf andere Websites unter Verwendung benutzerdefinierter Sperrseiten
- Implementierung konsistenter Sicherheit durch die transparente Bereitstellung der gleichen Richtlinien für alle Benutzer, ob lokal, mobil oder remote, über GlobalProtect.
- Nutzung einer bedingungslosen „Alles-andere-ablehnen“-Strategie oder die explizite Blockierung unerwünschter Anwendungen, wie P2P und Umgehungsprogramme oder Verkehr aus bestimmten Ländern, um den Anwendungsverkehr zu reduzieren, der Geschäfts- oder Sicherheitsrisiken mit sich bringen kann

Die Beispiele für die Aktivierung im Rechenzentrum – traditionell, virtualisiert oder eine Kombination daraus – konzentrieren sich auf die Bestätigung von Anwendungen, die Suche nach betrügerischen Anwendungen und den Schutz der Daten.

- Isolieren des Oracle-basierten Kreditkartennummern-Repositorys in seiner eigenen Sicherheitszone, Zugriffskontrolle für Gruppen aus der Buchhaltung, Erzwingen des Verkehrs über Standard-Ports und Überprüfung des Verkehrs auf Sicherheitslücken in den Anwendungen.



Einheitlicher Richtlinien-Editor: Das vertraute Aussehen und Verhalten des Regelwerks ermöglicht die schnelle Entwicklung und Implementierung von Richtlinien, die für Anwendungen, Benutzer und Inhalte definiert werden.



Transparenz von Inhalt und Risiken: Zeigt URL-Kategorien, Bedrohungen sowie die Anzahl von übertragenen Dateien/Daten in einem klaren und leicht zu interpretierenden Format an. Fügen Sie Filter hinzu oder entfernen Sie sie, um weitere Informationen zu einzelnen Elementen zu erhalten.

- Nur der IT-Gruppe gestatten, mit einer festen Palette verteilter Managementanwendungen (z. B. SSH, RDP, Telnet) über ihre Standard-Ports auf das Rechenzentrum zuzugreifen.
- Zulassen von Microsoft SharePoint Administration nur für Ihr Administrationsteam und Zulassen des Zugriffs auf Microsoft SharePoint Dokumente für alle anderen Benutzer.

Schutz zugelassener Anwendungen

Die sichere Aktivierung von Anwendungen bedeutet, den Zugriff auf bestimmte Anwendungen zuzulassen und anschließend bestimmte Richtlinien zur Blockierung bekannter Sicherheitslücken, Malware und Spyware (bekannt oder unbekannt) anzuwenden und den Datei- oder Datentransfer sowie die Surf-Aktivitäten im Internet zu kontrollieren. Häufige Umgehungsmethoden, wie Port-Hopping und Tunneling, werden durch die Ausführung von Richtlinien zum Schutz vor Bedrohungen, unschädlich gemacht. Dazu wird der Anwendungs- und Protokollkontext verwendet, der von Decodern in der App-ID erstellt wurde. Im Gegensatz dazu nutzen UTM-Lösungen bei jeder Funktion, Firewall, IPS, AV, URL-Filterung und Überprüfung des Verkehrs einen silobasierten Ansatz zum Schutz vor Bedrohungen, ohne Kontext freizugeben, wodurch das Risiko für die Ausnutzung von Schwachstellen erhöht wird.

- **Blockieren bekannter Bedrohungen: IPS und Netzwerk-Antivirus/Anti-Spyware.** Mithilfe eines einheitlichen Signaturformats und eines stream-basierten Scanning-Rechners können Sie Ihr Netzwerk vor einer Vielzahl an Bedrohungen schützen. Intrusion Prevention System (IPS)-Funktionen erkennen Sicherheitslücken in der Netzwerk- und Anwendungsschicht, verhindern Pufferüberläufe und Denial-of-Service-Attacken und hindern Port Scans daran, die Datenressourcen des Unternehmens zu gefährden und zu beschädigen. Antiviren/Anti-Spyware-Schutz blockiert Millionen von Malware-Varianten sowie durch Malware generierter „Command-and-Control"-Verkehr, unter anderem PDF-Viren und in komprimierten Dateien oder in Webverkehr verborgene Malware (komprimiertes HTTP/HTTPS). Eine auf Richtlinien basierende SSL-Entschlüsselung jeder Anwendung gestattet es den Unternehmen, sich gegen Malware zu schützen, die über SSL-verschlüsselte Anwendungen eindringt.
- **Blockieren unbekannter, spezialisierter Malware: Wildfire™.** Unbekannte oder zielgerichtete Malware wird von WildFire identifiziert und analysiert. Das Programm führt unbekannte Dateien direkt aus und überwacht diese in einer Cloud-basierten, virtualisierten Umgebung. WildFire überwacht mehr als 100 schädliche Funktionsweisen und das Ergebnis wird direkt in Form eines Alarms an den Administrator weitergegeben.

Durch ein optionales WildFire-Abonnement wird die Sicherheit, die Protokollierung und das Reporting verbessert. Wenn irgendwo auf der Welt eine neue Malware entdeckt wurde, sind Sie als Abonnent innerhalb von einer Stunde geschützt, wodurch die Ausbreitung der Malware effektiv verhindert wird, bevor Sie betroffen sind. Als Abonnent haben Sie außerdem Zugriff auf integrierte WildFire-Protokollierung und integriertes Reporting sowie eine API zur Übermittlung von Mustern zu Analysezwecken an die WildFire-Cloud.

- **Identifizieren von Bot-infizierten Hosts.** Die App-ID klassifiziert sämtliche Anwendungen über alle Ports hinweg, auch unbekannten Verkehr, der häufig zu Anomalien oder Bedrohungen in Ihrem Netzwerk führen kann. Der Botnet-Verhaltensbericht analysiert unbekannten Verkehr, verdächtige DNS- und URL-Anfragen und ungewöhnliches Netzwerkverhalten, um Geräte zu enttarnen, die möglicherweise mit Malware infiziert sind. Die Ergebnisse werden in Form einer Liste potenziell infizierter Hosts angezeigt, die als mögliche Elemente eines Botnet untersucht werden können.
- **Beschränkung unerlaubter Datei- und Datenübertragungen.** Die Datenfilterung gestattet Administratoren, Richtlinien zu implementieren, die die Risiken bei unerlaubten Datei- und Datenübertragungen minimieren. Dateiübertragungen können kontrolliert werden, indem die Datei (und nicht nur die Dateinamenerweiterung) überprüft wird, um festzustellen, ob der Transfer zugelassen werden sollte oder nicht. Ausführbare Dateien, die man typischerweise in Drive-by-Downloads findet, können blockiert werden, wodurch Ihr Netzwerk vor einer nicht erkannten Malware-Verbreitung geschützt wird. Datenfilterfunktionen können die Übertragung vertraulicher Datenmuster (Kreditkarten- und Sozialversicherungsnummern sowie benutzerdefinierte Muster) erkennen und kontrollieren.
- **Kontrolle des Websurfens.** Eine vollständig integrierte, anpassbare Engine für die URL-Filterung ermöglicht es Ihren Administratoren, präzise Richtlinien für das Surfen im Internet zu erstellen, die Anwendungstransparenz zu ergänzen, Richtlinien durchzusetzen und das Unternehmen vor einer ganzen Palette an rechtlichen, aufsichtsrechtlichen und der Produktivität abträglichen Risiken zu schützen. Zusätzlich können die URL-Kategorien in die Richtlinien integriert werden, um weitere Kontroll-Granularität für SSL-Entschlüsselung, QoS und andere Regelgrundlagen zu schaffen.

Fortlaufende Verwaltung und Analyse

Bewährte Vorgehensweisen im Bereich der Sicherheit fordern von den Administratoren einen Mittelweg zwischen einerseits aktiver Verwaltung der Firewall - ob für ein Gerät oder Hunderte - und reaktivem, investigativem Verhalten sowie dem Erstellen von Analysen und Berichten zu Sicherheitsvorfällen.

- **Verwaltung:** Jede Palo Alto Networks-Plattform kann individuell über eine Command Line Interface (CLI) oder voll funktionsfähige Browser-basierte Schnittstelle verwaltet werden. Panorama kann bei umfassenden Bereitstellungen lizenziert und als zentralisierte Verwaltungslösung genutzt werden, über die Sie einen Mittelweg zwischen globaler, zentralisierter Kontrolle und der Notwendigkeit für Flexibilität bei den lokalen Richtlinien finden können. Dazu werden Funktionen wie Vorlagen und gemeinsame Richtlinien verwendet. Durch die zusätzliche Unterstützung für normenbasierte Tools wie SNMP und REST-basierte APIs ist eine Integration in Verwaltungs-Tools von Drittanbietern möglich. Es macht keinen Unterschied, ob Sie die Weboberfläche des Geräts oder Panorama verwenden, das Aussehen und Verhalten der Oberfläche ist identisch, damit keine Lernkurve beim Wechsel entsteht. Ihre Administratoren können jederzeit über jede der Oberflächen Änderungen vornehmen, ohne sich über Synchronisierungsprobleme Gedanken machen zu müssen. Die rollenbasierte Administration wird in allen Verwaltungsmedien unterstützt, was die Zuweisung von Features und Funktionen zu bestimmten Personen möglich macht.
- **Reporting:** Vordefinierte Berichte können im Ist-Zustand verwendet, angepasst oder miteinander zu einem Report gruppiert werden, um den spezifischen Anforderungen zu entsprechen. Alle Berichte können ins CSV- oder PDF-Format exportiert und nach Zeitplan ausgeführt und per E-Mail versendet werden.
- **Protokollierung:** Protokollfilterung in Echtzeit ermöglicht eine schnelle forensische Untersuchung jeder Sitzung im Netzwerk. Protokolle der Filterergebnisse können zur Offline-Archivierung oder zur zusätzlichen Analyse in eine CSV-Datei exportiert oder an einen Syslog-Server gesendet werden.

Spezielle Hardware- oder virtualisierte Plattformen

Palo Alto Networks bietet eine vollständige Reihe an speziellen Hardware-Plattformen – von der PA-200 für Remote-Niederlassungen bis zu PA-5060 für Hochgeschwindigkeits-Rechenzentren. Die Plattformarchitektur basiert auf einer einzelnen Software. Diese verwendet eine funktionsspezifische Verarbeitung für Netzwerke, Sicherheit, Bedrohungsschutz und Management, um Ihnen vorhersehbare Leistung zu bieten. Die Firewall-Funktionen der Hardware-Plattformen sind auch in der virtuellen VM-Series-Firewall verfügbar. Darüber können Sie Ihre virtualisierten und Cloud-basierten Computerumgebungen mit den gleichen Richtlinien schützen, die auch auf Ihre Firewalls für Perimeter oder Remote-Büros angewendet werden.

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com