Übersicht der Firewallfunktionen

Die Produktfamilie aus Firewalls der nächsten Generation von Palo Alto Networks bietet ein beispielloses Maß an Transparenz und Kontrolle über Anwendungen, Benutzer und Inhalte im gesamten Unternehmensnetzwerk.

PA-4060

PA-4020

PA-4050

PA-2020

PA-2050

ANWENDUNGSIDENTIFIZIERUNG:

- Es können portübergreifend mehr als 700 Anwendungen unabhängig von Protokollen, SSL-Verschlüsselung oder Umgehungsmethoden identifiziert werden.
- Tools zur grafischen Darstellung ermöglichen einen einfachen und intuitiven Einblick in den Anwendungsdatenverkehr.
- Richtlinienkontrollen blockieren Malware und steuern erwünschte Anwendungen.

BENUTZERIDENTIFIZIERUNG:

- Richtlinienbasierte Transparenz und Kontrolle darüber, wer die Anwendungen verwendet, durch nahtlose Integration von Microsoft Active Directory (AD)
- Kontrolle von Nicht-Windows-Hosts per webbasierter Authentifizierung

INHALTSIDENTIFIZIERUNG:

- Blockieren von Viren, Spyware und Exploits für Sicherheitslücken, Begrenzen von nicht autorisierten Übertragungen von Dateien und vertraulichen Daten wie Kreditkartennummern und Kontrollieren der Internetnutzung für private Zwecke
- Einzeldurchlaufarchitektur ermöglicht Multi-Gigabit-Durchsatz bei kurzer Latenzzeit während der Inhaltsüberprüfung

PLATTFORMUNTERSTÜTZUNG UND FIREWALLDURCHSATZ:

- PA-4060 - 10 GBit/s
- PA-4050 - 10 GBit/s
- PA-4020 - 2 GBit/s
- PA-2050 - 1 GBit/s
- PA-2020 - 500 MBit/s

paloalto NETWORKS

Als Herzstück der Unternehmensnetzwerk-Sicherheit ist die Firewall der ideale Ansatzpunkt zum Durchsetzen von Sicherheitsrichtlinien. Da herkömmliche Firewalls für die Datenverkehrsklassifizierung jedoch von Ports und Protokollen abhängig sind, können aktuelle Internetanwendungen diese ohne Weiteres umgehen, indem sie auf Port-Hopping und SSL-Verschlüsselung zurückgreifen, über Port 80 eindringen oder nicht standardisierte Ports nutzen, die meist offen gelassen werden. Der daraus resultierende Kontrollverlust über Anwendungen setzt Unternehmen geschäftskritischen Risiken aus, beispielsweise Netzwerkausfallzeiten, höhere Betriebsausgaben und Datenverlust durch unautorisierte Datenübertragung.

Eine Firewall der nächsten Generation stellt die Transparenz von Anwendungen und deren Kontrolle in modernen Unternehmen wieder her und überprüft Anwendungsinhalte auf Sicherheitsrisiken. So werden Unternehmen in die Lage versetzt, ein effizienteres Risikomanagement zu betreiben. Unternehmen benötigen eine Firewall der nächsten Generation, die folgende wichtige Anforderungen erfüllt:

- Portübergreifende Identifikation von Anwendungen, unabhängig von Protokollen, SSL-Verschlüsselung oder Umgehungsmethoden
- Echtzeitschutz vor Angriffen und im Anwendungsverkehr aktiver Malware
- Vereinfachte Richtlinienverwaltung mithilfe von leistungsstarken Visualisierungstools und einem Editor für einheitliche Richtlinien
- Multi-Gigabit-Durchsatz ohne Leistungsbeeinträchtigungen bei Inline-Implementierung

Die Firewall der nächsten Generation von Palo Alto Networks™ zielt auf die maßgeblichen Schwächen von herkömmlichen Firewalls mit zustandsgesteuerter Filterung (Stateful Inspection) ab und bringt richtlinienbasierte Transparenz und Kontrolle über Anwendungen, Benutzer und Inhalte wieder zurück in die IT-Abteilung, wo sie hingehören.

Identifikationstechnologien: Die Stärke der Firewall der nächsten Generation von Palo Alto Networks

Die Produktfamilie aus Firewalls der nächsten Generation von Palo Alto Networks bietet richtlinienbasierte Transparenz und Kontrolle über Anwendungen mithilfe von drei einzigartigen Identifikationsmethoden: App-ID, User-ID und Content-ID.

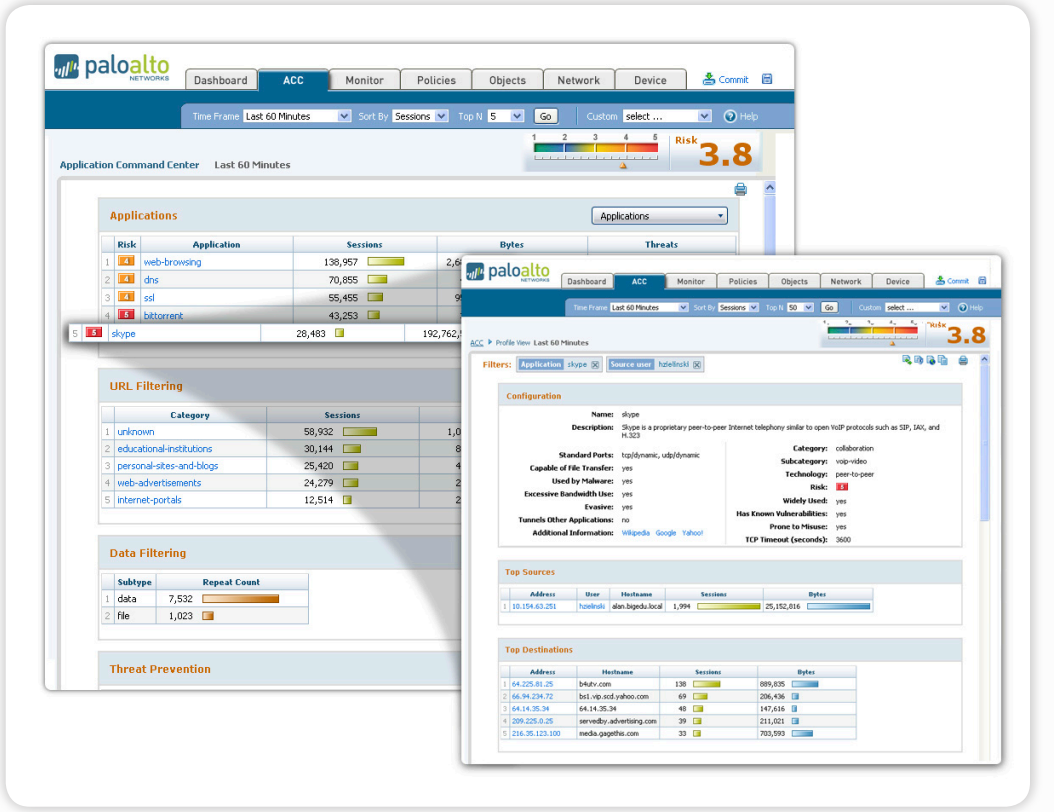
- **App-ID** ist eine zum Patent angemeldete Technologie zur Datenverkehrsklassifizierung, mit der genau bestimmt werden kann, welche Anwendungen im Netzwerk verwendet werden. Dabei werden bis zu vier verschiedene Identifizierungsmethoden angewendet. Die Anwendungsidentität wird dann als Grundlage für alle Richtlinienentscheidungen herangezogen, einschließlich der ordnungsgemäßen Verwendung und Inhaltsfilterung.
  - **Anwendungsprotokollerkennung und -entschlüsselung:** Anhand umfassender Informationen zu Anwendungsprotokollen bestimmt App-ID, welches Protokoll verwendet wird und ob es SSL-verschlüsselt ist. Verschlüsselte Daten werden entschlüsselt und richtliniengemäß gefiltert, wieder verschlüsselt und versendet.
  - **Anwendungsprotokolldecodierung:** Protokolldecoder bestimmen, ob die Anwendung ein Protokoll für den normalen Anwendungstransport oder zur Verschleierung verwendet, und sie dienen dazu, die Zahl der fraglichen Anwendungen einzugrenzen, indem sie bei der Anwendung von Signaturen hilfreichen Kontext bereitstellen. Die Decoder ermitteln darüber hinaus Dateien und andere Inhalte, die auf Sicherheitsrisiken oder vertrauliche Daten überprüft werden sollten.
  - **Anwendungssignaturen:** Bei kontextbasierten Signaturen wird nach eindeutigen Anwendungseigenschaften und ähnlichen Transaktionsmerkmalen gesucht, um die Anwendung richtig und unabhängig vom verwendeten Protokoll oder Port zu identifizieren.
  - **Heuristik:** Die heuristische Analyse oder Verhaltensanalyse wird je nach Bedarf mit anderen App-ID-Identifizierungstechniken kombiniert, um bestimmte Anwendungen mit Umgehungsmethoden zu identifizieren, insbesondere solche, die eine proprietäre Verschlüsselung verwenden.

App-ID
Komponenten zur mehrfachen Datenverkehrsklassifizierung identifizieren präzise die Anwendungen im Netzwerk.

- **User-ID** sorgt für eine nahtlose Integration von Firewalls der nächsten Generation von Palo Alto Networks und Active Directory, um eine IP-Adresse dynamisch mit Benutzer- und Gruppeninformationen verknüpfen zu können. Mithilfe von Transparenz bezüglich der Benutzeraktivitäten können Unternehmen Anwendungen und Inhalte im Netzwerk anhand der im Benutzerrepository gespeicherten Benutzer- und Gruppeninformationen überwachen und kontrollieren.
- **Content-ID** verbindet eine Komponente für den Echtzeitschutz vor Sicherheitsrisiken mit einer umfassenden URL-Datenbank und Elementen zur Anwendungsidentifizierung, um nicht autorisierte Dateiübertragungen einzugrenzen, zahlreiche Sicherheitsrisiken zu erkennen und zu blockieren und die Internetnutzung für private Zwecke zu kontrollieren. Eine Single-Pass-Architektur filtert den Datenverkehr mithilfe einer Kombination aus Stream-basierter Überprüfung und einem einheitlichen Signaturformat. Content-ID wird in Verbindung mit App-ID eingesetzt, um anhand der Anwendungsidentität eine noch wirksamere Inhaltsfilterung zu ermöglichen.

Eine umfassende Palette an Netzwerk-, IPSec-VPN- und Verwaltungsfunktionen ergänzen mit App-ID, User-ID und Content-ID die Kernfunktionen des PAN-Betriebssystems. Dieses sicherheitsorientierte Betriebssystem steuert Firewalls der nächsten Generation von Palo Alto Networks. Das PAN-Betriebssystem ist für unterschiedliche anpassbare Hardwareplattformen vorgesehen, die die Verwaltung des Datenverkehrs in Unternehmensnetzwerken mithilfe von funktionsspezifischer Verarbeitung für Netzwerk, Sicherheit, Schutz vor Sicherheitsrisiken und Verwaltungsaufgaben fördern.

Application Command Center
Zeigen Sie aktuelle Aktivitäten im Zusammenhang mit Anwendungen, URLs, Datenfilterung und Sicherheitsrisiken in einem klaren und leicht zu interpretierenden Format an. Fügen Sie Filter hinzu/Entfernen Sie Filter, um Daten bis ins kleinste Detail anzuzeigen.



Leistungsstarke Visualisierungstools

Leistungsstarke Visualisierungstools bieten Administratoren die Möglichkeit, zahlreiche Datenpunkte bei Anwendungen im Netzwerk anzuzeigen, ebenso wie die Benutzer, die diese verwenden, und die potenziellen Auswirkungen auf die Sicherheit. Das Application Command Center (Anwendungskontrollcenter), der Log-Viewer und die vollständig anpassbare Berichterstellung sind die primären Komponenten der Weboberfläche, die den Administratoren eine beispiellose Transparenz bezüglich Anwendungen, Benutzern und Inhalten im Netzwerk bieten.

- **Application Command Center (ACC):** ACC stellt Anwendungen, URLs, Sicherheitsrisiken und Daten (Dateien und Muster) im Netzwerk grafisch dar. Im Gegensatz zu anderen Lösungen, bei denen die Daten möglicherweise in einem kryptischen und schwer lesbaren Format angezeigt werden, ermöglicht ACC Administratoren einen Einblick in die aktuellen Aktivitäten. Diese Ansicht kann auf sieben verschiedene Weisen angepasst werden.
  - Die Anwendungsdaten können nach Risiko, Kategorie, Unterkategorie oder zugrunde liegender Technologie angezeigt werden.
  - Webaktivitäten können nach den am häufigsten aufgerufenen oder blockierten URLs oder am häufigsten aufgerufenen oder blockierten URL-Kategorien angezeigt werden.
  - Mithilfe der Datenfilterung werden Dateien und Muster von vertraulichen Daten (z. B. Kreditkartennummern) im Netzwerk angezeigt.
  - Aktivitäten im Zusammenhang mit Sicherheitsrisiken können basierend auf Spyware, Exploits für Sicherheitslücken und Viren angezeigt werden.

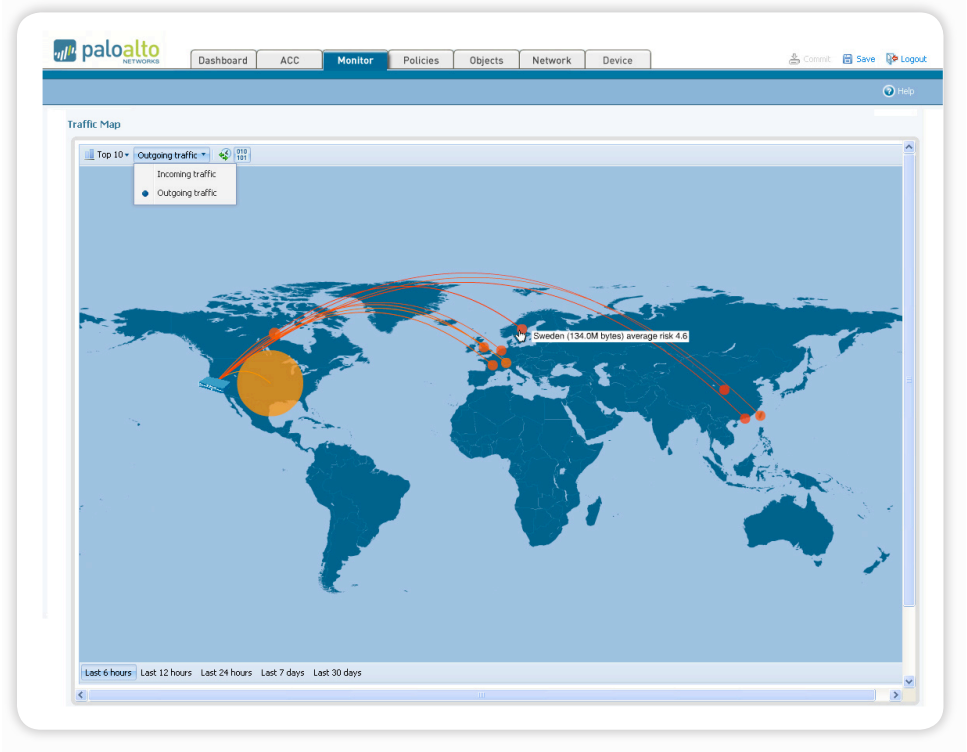
Um weitere Informationen zu den Anwendungen, URLs, Daten und Sicherheitsrisiken im Netzwerk zu erhalten, können Administratoren ACC-Daten durchsuchen, indem sie Filter hinzufügen oder entfernen und so die gewünschten Ergebnisse erzielen. Beispielsweise kann durch Auswahl einer bestimmten Anwendung angezeigt werden, von wem sie verwendet wird, wohin der Datenverkehr fließt und welches die Quell- und Zielländer sind. Es können zusätzliche Filter hinzugefügt werden, um detailliertere Informationen zum Verhalten einzelner Benutzer, zu den Sicherheitszonen, die den Datenverkehr senden und empfangen, zu potenziellen Sicherheitsrisiken und zur Art der übertragenen Dateien oder Datentypen zu erhalten. Aufgrund der Transparenz, die das Data Mining über das ACC ermöglicht, können Administratoren Details zu den Netzwerkaktivitäten erfahren, um sie richtlinienbezogenen Entscheidungen zugrunde zu legen oder um schneller auf potenzielle Sicherheitsrisiken zu reagieren. Weist das ACC auf Situationen hin, die eine sofortige detaillierte Analyse erfordern, können Administratoren einfach per Mausklick zu den Protokollen wechseln, die dem aktuellen ACC-Kontext entsprechen.

- **Berichterstellung und Protokollierung:** Der Log-Viewer ermöglicht forensische Untersuchungen jeder Sitzung im Netzwerk mithilfe von Echtzeitfiltern und regulären Ausdrücken. Es sind vollständig anpassbare und planbare Berichte verfügbar, die einen detaillierten Einblick bezüglich Anwendungen, Benutzern und Sicherheitsrisiken im Netzwerk bieten.

Inhaltsfilterung:

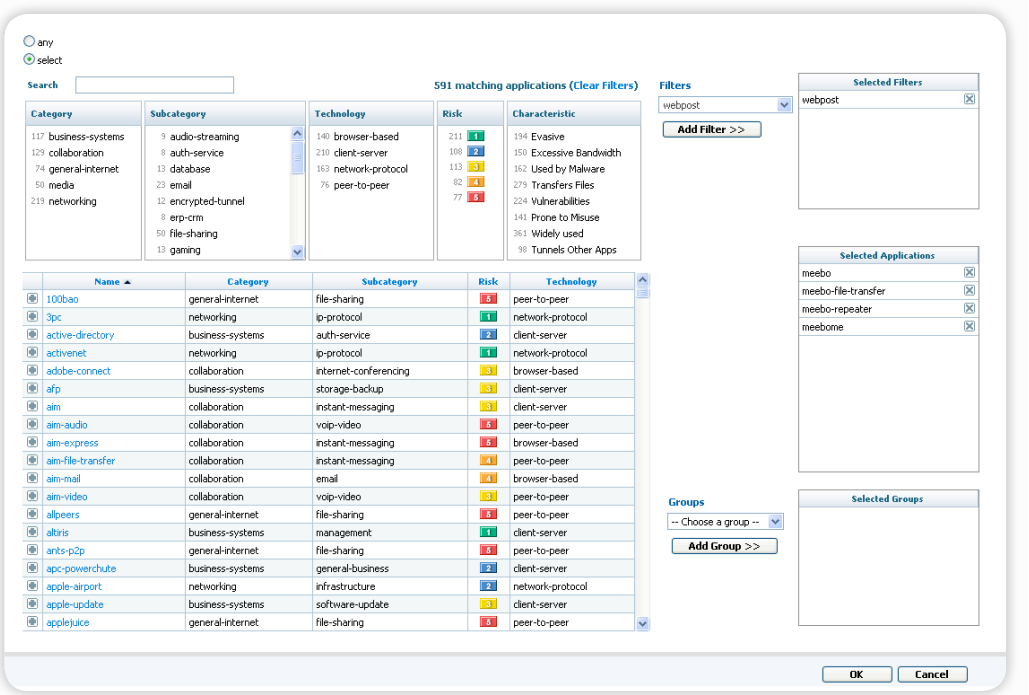
Durch die präzise Identifikation von Anwendungen mithilfe von App-ID können Anforderungen, die sich bezüglich Transparenz und Kontrolle den IT-Abteilungen stellen, mit heutzutage vorwiegend webbasierten Umgebungen nur zum Teil erfüllt werden. Die Filterung des zugelassenen Anwendungsdatenverkehrs ist eine der nächsten großen Herausforderungen; ihr wird durch Content-ID mit Schutz vor Sicherheitsrisiken, URL-Filterung und Elementen zur Datenfilterung begegnet.

- **URL-Filterung:** Eine vollständig integrierte Datenbank zur URL-Filterung mit mehr als 20 Millionen URLs aus 76 Kategorien ermöglicht es Administratoren, präzise Richtlinien für das Browsen im Web anzuwenden, um damit die Richtlinien für Anwendungstransparenz und -kontrolle zu ergänzen und das Unternehmen vor zahllosen Risiken im Zusammenhang mit der Einhaltung gesetzlicher Bestimmungen, der Produktivität und der Ressourcen zu schützen. Zusätzlich zu den Optionen, die der Einsatz von schwarzen oder weißen Listen bietet, können Administratoren auch anpassbare Sperrseiten verwenden sowie kennwortgeschützen Zugriff und Außerkraftsetzungen durch Benutzer einrichten, um flexible und dennoch erzwingbare Richtlinien für Webaktivitäten umzusetzen.
- **Schutz vor Sicherheitsrisiken:** Das Erkennen und Blockieren zahlreicher Sicherheitsrisiken wie Viren, Spyware und Exploits für Sicherheitslücken in Anwendungen werden von einer Komponente gewährleistet, die Echtzeitschutz durch die Single-Pass-Architektur von Palo Alto Networks bietet. Bei dieser Komponente wird ein einheitliches Signaturformat mit Stream-basierter Überprüfung kombiniert, um den Datenverkehr einmalig zu filtern, wobei in einem einzelnen Durchlauf alle Arten von Malware gleichzeitig erkannt und blockiert werden. Aufgrund der Single-Pass-Architektur ist es nicht mehr erforderlich, die Dateien vor der Filterung nach Sicherheitsrisiken zu puffern oder über einen Proxy zu senden, was erhöhten Durchsatz und kürzere Latenzzeit ermöglicht.
- **Datei- und Datenfilterung:** Indem Administratoren die umfassende Anwendungsfilterung durch App-ID und die Einzeldurchlaufarchitektur in vollem Umfang ausschöpfen, können sie mehrere unterschiedliche Arten von Richtlinien implementieren, um die mit der nicht autorisierten Datenübertragung verbundenen Risiken zu minimieren.
  - **Dateiblockierung nach Typ:** Mithilfe dieser Blockierung wird der Umlauf zahlreicher Dateitypen kontrolliert. Dabei wird das Datenaufkommen genau untersucht, um den Dateityp zu identifizieren, anstatt dazu lediglich die Dateierweiterung zu nutzen.
  - **Datenfilterung:** Bei dieser Filterung wird die Übertragung von Mustern vertraulicher Daten identifiziert und kontrolliert, z. B. von Kreditkartennummern in Anwendungsinhalten oder Anhängen.
  - **Steuerung der Dateiübertragungsfunktion:** Diese Steuerung ermöglicht es, die Dateiübertragungsfunktionalität in einzelnen Anwendungen zu kontrollieren. Dabei können die Anwendungen genutzt und gleichzeitig unerwünschte eingehende oder ausgehende Dateiübertragungen unterbunden werden.



Grafische Darstellung des Datenverkehrs
Geografische Darstellung des Datenverkehrs und der Sicherheitsrisiken innerhalb und außerhalb des Netzwerks

Anwendungsbrowser
Weitere Informationen zu den Anwendungen im Netzwerk und zum sofortigen Einbezug der Ergebnisse in Sicherheitsrichtlinien



Richtlinienbasierte Kontrolle:

Die stärkere Transparenz von Netzwerkaktivitäten durch App-ID, User-ID und Content-ID ermöglicht es Sicherheitsspezialisten, die Anwendungen im Netzwerk schnell zu erfassen und zu erfahren, wer sie verwendet und welche potenziellen Sicherheitsrisiken bestehen, um diese Informationen dann problemlos in ihre Firewallrichtlinien einzubeziehen. Die anwendungsbasierte Richtlinienkontrolle wird mithilfe des Anwendungsbrowsers aktiviert, einem integralen Bestandteil des Richtlinien-Editors, mit dem Administratoren umfassende Informationen anzeigen können, die für Entscheidungen zum Einsatz einer Anwendung relevant sind. Der Richtlinien-Editor weist ein vertrautes Aussehen und Verhalten auf, wodurch erfahrenere Firewalladministratoren schnell Firewallrichtlinien wie die folgenden erstellen können:

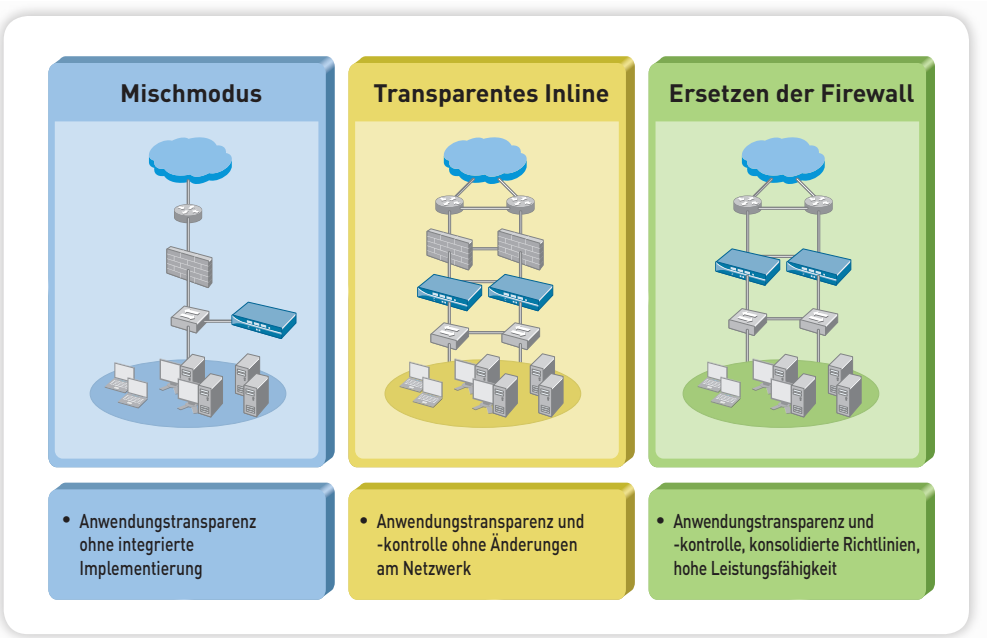
- Verweigern des Zugriffs auf bestimmte Anwendungstypen wie Peer-to-Peer-Anwendungen oder Umgehungsprogramme und Proxydienste
- Zuweisen von Saleforce.com und Oracle zu den Vetriebs- und Marketinggruppen wie in Active Directory festgelegt. Festlegen einer Gruppe von Anwendungen wie SSH, Telnet und MS-RDP und ausschließliches Zulassen der Verwendung durch die IT-Gruppe
- Festlegen und Erzwingen einer Unternehmensrichtlinie, die bestimmt, welche Webmail- und Instant-Messaging-Anwendungen verwendet werden können, und die diese auf Viren, Spyware und Exploits für Sicherheitslücken überprüft – alles über eine einzige Richtlinienregel
- Identifizieren der Übertragung von vertraulichen Informationen wie Kreditkartennummern, entweder im Text- oder Dateiformat, und Blockieren, Zulassen oder Senden von Benachrichtigungen dazu, wer die Daten überträgt
- Festlegen von Richtlinien für die Filterung von URLs auf mehreren Ebenen, die den Zugriff auf offensichtlich für private Zwecke genutzte Websites blockieren, die fraglichen Websites überwachen und den Zugriff auf andere Websites „trainieren“, indem sie dem Benutzer nach Anzeige einer ersten Warnung die Möglichkeit zum Fortfahren bieten
- Erstellen von herkömmlichen Firewallregeln für den eingehenden und ausgehenden portbasierten Datenverkehr kombiniert mit anwendungsbasierten Regeln für den reibungslosen Wechsel zu einer Firewall der nächsten Generation von Palo Alto Networks

Netzwerk

Eine flexible Netzwerkarchitektur, die dynamisches Routing, Switching, hohe Verfügbarkeit sowie IPSec-VPN-Unterstützung umfasst und die Bereitstellung in nahezu jeder Netzwerkumgebung ermöglicht.

- **Virtual Wire:** Virtual Wire verbindet zwei Ports logisch miteinander und leitet sämtlichen Datenverkehr an den anderen Port ohne Switching oder Routing weiter und ermöglicht eine vollständige Filterung und Kontrolle ohne Auswirkungen auf die Geräte in der Umgebung. Mehrere Virtual-Wire-Paare können für die Unterstützung mehrerer Netzwerksegmente konfiguriert werden.
- **Switching und Routing:** Netzwerkfunktionen ähnlich denen üblicher L2-/L3-Architekturen, aber mit zonenbasierter Sicherheitserzwingung, ermöglichen eine Bereitstellung in L2-/L3-Netzwerken. Dynamische Routingprotokolle (OSPF und RIP) in Kombination mit umfassender 802.1Q VLAN-Unterstützung werden sowohl für L2 als auch L3 bereitgestellt, sodass alle Dienste ohne Auswirkung auf die vorhandene Routing- oder VLAN-Architektur aktiviert werden können.

Optionen für die flexible Bereitstellung
Umfangreiche Netzwerkfunktionen ermöglichen eine Bereitstellung als Ergänzung oder Ersatz für eine vorhandene Firewall.



- **Hohe Verfügbarkeit:** Aktive/passive hohe Verfügbarkeit wird unterstützt, wo ein aktives Gerät seine Konfigurations- und Sitzungsinformationen kontinuierlich mit einem passiven Gerät synchronisiert.
- **VPN zwischen Standorten:** Standardbasierte IPSec-VPN-Konnektivität kombiniert mit Anwendungstransparenz und -kontrolle ermöglicht die geschützte Kommunikation zwischen zwei oder mehr Geräten von Palo Alto Networks bzw. IPSec-VPN-Geräten von anderen Anbietern.

Verwaltung:

Um den dynamischen Anforderungen von Netzwerksicherheit und den unterschiedlichen Verwaltungsarten und -rollen gerecht zu werden, die vom jeweiligen Administrator abhängen, können alle Firewalls von Palo Alto Networks über eine Befehlszeilenschnittstelle gesteuert werden. Dabei handelt es sich um eine webbasierte Schnittstelle oder eine zentralisierte Verwaltungslösung (Panorama) mit anpassbaren Rollen, die den Zugriff auf die für den jeweiligen Administrator notwendigen Verwaltungsfunktionen beschränken. Der Wechsel von einer Verwaltungsschnittstelle zu einer anderen erschwert die Verwaltungsarbeiten nicht, da immer die aktuellste Konfiguration eingesetzt und so die Verwendung durch nicht synchronisierte Konfigurationen unterbunden wird. Panorama und webbasierte Schnittstelle gleichen sich in Aussehen und Verhalten. So verringert sich der Lernaufwand, der häufig mit dem Wechsel zwischen Schnittstellen zur Verwaltung von einzelnen Geräten und zentralisierten Schnittstellen verbunden ist. Vervollständigt werden die Verwaltungsschnittstellen mit standardbasierten Syslog- und SNMP-Schnittstellen.

Berichterstellung und Protokollierung:

Der rasche Zugriff auf leistungsstarke Tools zur Berichterstellung und Protokollierung ermöglicht die Analyse von Sicherheitsvorfällen, Anwendungseinsätzen und Datenverkehrsmustern.

- **Anpassbare Berichte:** Erstellen Sie neue anpassbare Berichte, die Daten aus einer beliebigen Protokolldatenbank heranziehen, oder bearbeiten Sie einen der vordefinierten Berichte.
- **Exportieren von Berichten:** Exportieren Sie einen beliebigen vordefinierten oder anpassbaren Bericht in eine CSV- oder PDF-Datei. Alle Berichte im PDF-Format können nach Zeitplan per E-Mail gesendet werden.
- **Zusammenfassungsbericht:** Eine anpassbare, eine einzelne Seite umfassende Zusammenfassung, die auf Daten aus einem der vordefinierten oder anpassbaren Berichte zurückgreift und nach Zeitplan erstellt und per E-Mail gesendet werden kann.
- **Log-Viewer:** Zeigen Sie Aktivitäten im Zusammenhang mit Anwendungen, Sicherheitsrisiken und Benutzern mithilfe von dynamischen Filterfunktionen an, die einfach aktiviert werden können, indem Sie auf einen Wert in einer Zelle klicken und/oder die Filterkriterien mithilfe des Ausdrucks-Generators festlegen.
- **Exportieren von Protokollen:** Exportieren Sie ein beliebiges Protokoll, das dem aktuellen Filter entspricht, zur Offline-Archivierung oder zur zusätzlichen Analyse in eine CSV-Datei.

paloalto NETWORKS

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA. 94089
Vertrieb +1 866 207 0077
www.paloaltonetworks.com

840-000001-00A