

# Übersicht der Firewallfunktionen

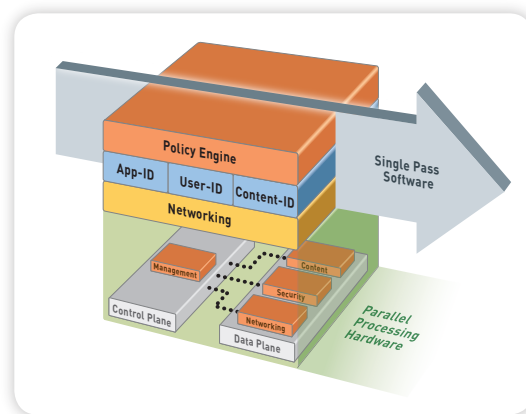
Eine Firewall der nächsten Generation stellt die Transparenz von Anwendungen und deren Kontrolle in modernen Unternehmen wieder her und überprüft Anwendungsinhalte auf Sicherheitsrisiken. So werden Unternehmen in die Lage versetzt, ein effizienteres Risikomanagement zu betreiben. Zu den wichtigen Anforderungen an Firewalls der nächsten Generation gehören folgende Möglichkeiten:

- Portübergreifende Identifikation von Anwendungen, unabhängig von Protokollen, SSL-Verschlüsselung oder Umgehungsmethoden.
- Richtlinienkontrolle nach Benutzeridentität und/oder Gruppenzugehörigkeit, nicht nur nach der IP-Adresse.
- Echtzeitschutz vor Angriffen und im Anwendungsverkehr aktiver Malware.
- Vereinfachte Richtlinienverwaltung mithilfe von leistungsstarken Visualisierungstools und eines Editors für einheitliche Richtlinien.
- Multi-Gigabit-Durchsatz ohne Leistungsbeeinträchtigungen bei Inline-Implementierung.

Die Firewall ist der strategisch wichtigste Teil der Infrastruktur; sie erkennt den gesamten Datenverkehr und ist daher der ideale Ansatzpunkt zum Durchsetzen von Sicherheitsrichtlinien. Leider sind herkömmliche Firewalls für die Datenverkehrsklassifizierung jedoch von Ports und Protokollen abhängig, wodurch intelligente Anwendungen und Benutzer mit Computererfahrung diese ohne Weiteres umgehen können, indem sie auf Port-Hopping und SSL-Verschlüsselung zurückgreifen, über Port 80 eindringen oder nicht standardisierte Ports nutzen.

Der daraus resultierende Kontrollverlust setzt Unternehmen Netzwerkausfallzeiten, Verstößen gegen die Konformität, höheren Betriebsausgaben und möglichem Datenverlust aus. Der herkömmliche Ansatz zur Lösung dieses Problems erforderte, dass hinter der Firewall zusätzliche „Firewall-Helfer“ implementiert werden. Aufgrund begrenzter Transparenz des Datenverkehrs, umständlicher Verwaltung, durch Multi-Scan-Software verursachter Latenzzeiten und geringen Durchsatzes löst dieser kostspielige Ansatz das Problem nicht.

Firewalls der nächsten Generation von Palo Alto Networks™ bringen hohe Leistungsfähigkeit, richtlinienbasierte Transparenz und Kontrolle über Anwendungen, Benutzer und Inhalte zurück zur Firewall – dorthin, wo sie hingehören.



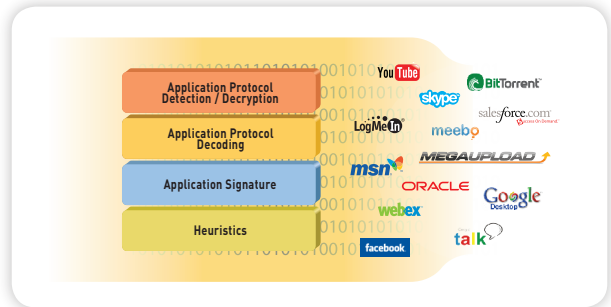
Single-Pass-Parallel-Processing-Architektur

Die Grundlage der Firewall der nächsten Generation von Palo Alto Networks ist eine Single-Pass-Parallel-Processing-Architektur, ein einzigartiger Ansatz, Software und Hardware zu integrieren, der die Verwaltung vereinfacht, die Verarbeitung rationalisiert und die Leistung maximiert. Die Single-Pass-Software führt gleichzeitig eine Richtlinienuche, die Anwendungsidentifizierung und -decodierung, die Zuordnung der Active-Directory-Benutzer und eine Inhaltsüberprüfung (Viren, Spyware, IPS - Schutz vor unbefugtem Zugriff) für eine gegebene Datenverkehrsmenge aus. Die Software ist direkt verbunden mit einer parallel arbeitenden Hardwareplattform, die funktionspezifische Prozessoren für Netzwerk, Sicherheit, Schutz vor Sicherheitsrisiken und Verwaltungsaufgaben verwendet und so den Durchsatz maximiert und Latenzzeiten minimiert.

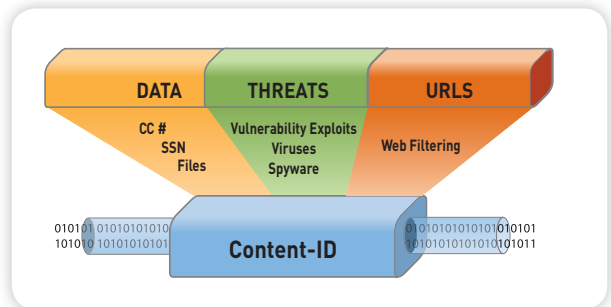
**Einzigartige Erkennungstechniken ermöglichen Transparenz und Kontrolle**

Die drei wichtigsten Elemente der Single-Pass-Parallel-Processing-Architektur, die Transparenz und Kontrolle über Anwendungen, Benutzer und Inhalte ermöglichen, sind App-ID, User-ID und Content-ID. Mithilfe dieser einzigartigen Identifikationstechnologien können IT-Manager exakt bestimmen, was in ihrem Netzwerk geschieht; dadurch können sie fundiertere Richtlinienentscheidungen treffen und ihre Sicherheitslage verbessern.

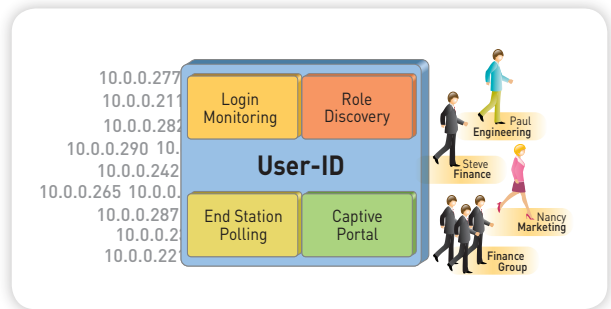
- **App-ID:** Mithilfe von nicht weniger als vier verschiedenen Mechanismen zur Datenverkehrsklassifizierung identifiziert App-ID™ exakt, welche Anwendungen genau im Netzwerk ausgeführt werden, unabhängig vom Port, vom Protokoll, von der SSL-Verschlüsselung oder von der Umgehungsmethode, die verwendet werden. App-ID bietet Administratoren stärkere Transparenz über die tatsächliche Identität der Anwendung, wodurch sie umfassende Richtlinien für die Kontrolle der Anwendungseinsätze sowohl für den eingehenden als auch für den ausgehenden Datenverkehr aufstellen können.



- **Content-ID:** Ein Stream-basiertes Überprüfungsmodul, das ein einheitliches Format für Bedrohungssignaturen verwendet, erkennt und blockiert zahlreiche Sicherheitsrisiken und begrenzt nicht autorisierte Übertragungen von Dateien und vertraulichen Daten. Gleichzeitig kontrolliert eine URL-Datenbank Internetnutzung für private Zwecke. Darüber hinaus bietet User-ID Transparenz über Citrix- und Terminal-Services-Umgebungen und ermöglicht vollständige Anwendungstransparenz, Entwicklung von Richtlinien, Protokollierung und Berichterstellung.



- **User-ID:** Die nahtlose Integration von Microsoft Active Directory verknüpft die IP-Adresse mit bestimmten Benutzer- und Gruppeninformationen. So werden IT-Organisationen in die Lage versetzt, Anwendungen und Inhalte anhand der im Microsoft Active Directory gespeicherten Mitarbeiterinformationen zu überwachen. Mithilfe von User-ID können Administratoren Benutzer- und Gruppendaten zur Anwendungstransparenz, zur Entwicklung von Richtlinien, zur Protokollierung und zur Berichterstellung nutzen.

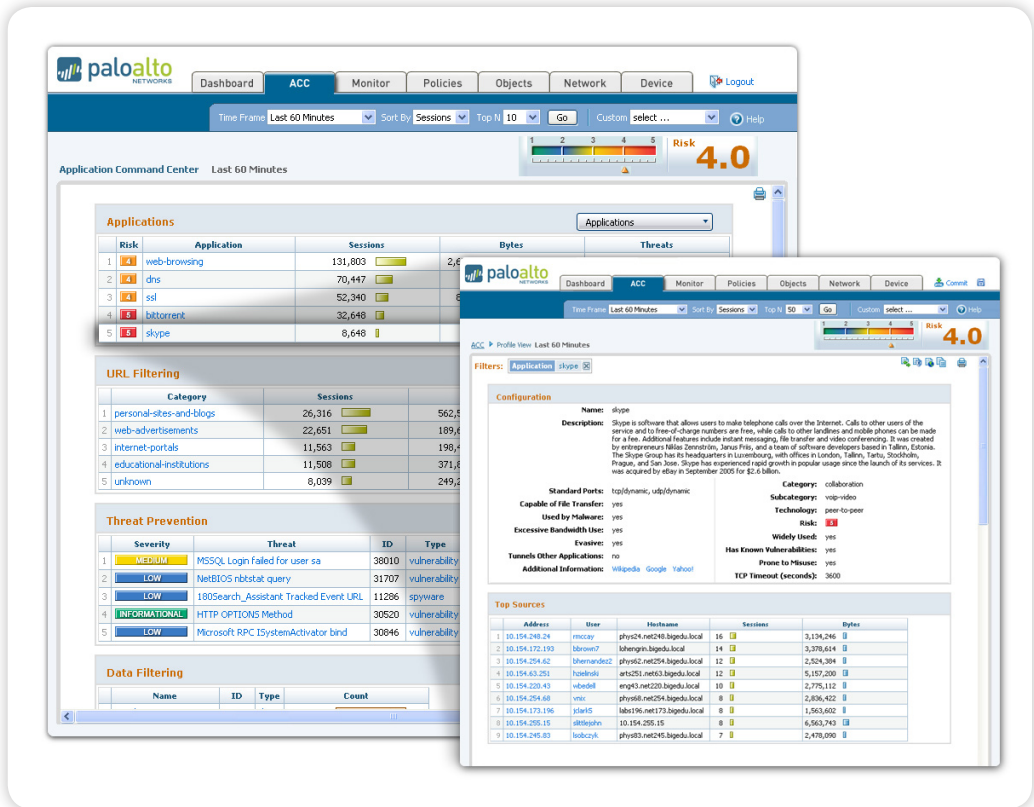


Vervollständigt werden die Funktionen des PAN-Betriebssystems, des sicherheitsorientierten Betriebssystems, das die Firewalls der nächsten Generation von Palo Alto Networks steuert, durch eine umfassende Palette an traditionellen Firewall-, Management- und Netzwerkfunktionen.

Weitere Informationen zu den Identifikationstechnologien von Palo Alto Networks finden Sie auf der Website <http://www.paloaltonetworks.com/technology/index.html>

**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 Visualisierungs- und Verwaltungstools**

Eine leistungsstarke Palette an Visualisierungstools wie dem Application Command Center (ACC, Anwendungskontrollcenter), App-Scope, dem Log-Viewer und der vollständig anpassbaren Berichterstellung bietet Sicherheitsadministratoren die Möglichkeit, zahlreiche Datenpunkte bei Anwendungen im Netzwerk ebenso anzuzeigen wie die Benutzer, die diese verwenden, und die potenziellen Auswirkungen auf die Sicherheit.

- **Application Command Center (ACC):** ACC stellt einen aktuellen Einblick in Anwendungen, URLs, Sicherheitsrisiken und Daten (Dateien und Muster) im Netzwerk grafisch dar. Ein Administrator kann eine Anwendung mithilfe von Filtern daraufhin untersuchen, welche Mitarbeiter diese Anwendung verwenden und welche Sicherheitsrisiken dadurch für das Netzwerk entstehen können. Es können zusätzliche Filter hinzugefügt werden, um detailliertere Informationen zum Verhalten einzelner Benutzer, zu Sicherheitsrisiken und zu den damit verbundenen Datenverkehrsmustern zu erhalten. Aufgrund der Transparenz, die das Data Mining über das ACC ermöglicht, können Administratoren fundiertere richtlinienbezogene Entscheidungen treffen oder schneller auf potenzielle Sicherheitsrisiken reagieren.

- **App-Scope:** App-Scope ergänzt den aktuellen Einblick in den Datenverkehr, den ACC präsentiert, durch ein dynamisches, vom Benutzer anpassbares Fenster mit Blick auf die Netzwerkaktivität, mit dem Administratoren durch einen Einblick über das, was sich im Laufe der Zeit ereignet hat, problematisches oder unregelmäßiges Verhalten genau lokalisieren können.
- **Protokollierung und Berichterstellung:** Der Log-Viewer ermöglicht forensische Untersuchungen jeder Sitzung im Netzwerk mithilfe von Echtzeitfiltern und regulären Ausdrücken. Vordefinierte, vollständig anpassbare und planbare Berichte bieten einen detaillierten Einblick bezüglich Anwendungen, Benutzern und Sicherheitsrisiken im Netzwerk.
- **Management:** Das Management der Firewall von Palo Alto Networks ist über eine Befehlszeilenschnittstelle, eine webbasierte Schnittstelle oder eine zentralisierte Verwaltungslösung (Panorama) möglich. In Umgebungen, in denen verschiedene Mitarbeiter unterschiedliche Zugangsstufen für die Verwaltungsschnittstelle benötigen, ermöglicht eine funktionsabhängige Verwaltung über alle drei Verwaltungsmechanismen hinweg die Delegation administrativer Funktionen an die geeignete Person. Vervollständigt werden die Verwaltungsschnittstellen durch standardbasierte Syslog- und SNMP-Schnittstellen.

### Richtlinienbasierte Kontrollen ermöglichen die ordnungsgemäße Verwendung von Anwendungen

Die stärkere Transparenz von Netzwerkaktivitäten durch App-ID, User-ID und Content-ID kann die Aufgabe vereinfachen zu bestimmen, welche Anwendungen im Netzwerk ausgeführt werden, wer sie verwendet und welche potenziellen Sicherheitsrisiken bestehen, um dann problemlos die geeignete Reaktion festzulegen. Mit diesen Datenpunkten ausgestattet, können Administratoren Richtlinien mit einer Vielzahl von Reaktionen anwenden, die genauere Abstufungen erlauben als nur „zulassen“ oder „verweigern“. Zu den Reaktionen der Richtlinienkontrolle gehören:

- Zulassen oder verweigern
- Zulassen, aber überprüfen
- Zulassen gemäß Zeitplan
- Entschlüsseln und prüfen
- Optimierung der Kapazitätsauslastung anwenden
- Beliebige Kombination
- Bestimmte Anwendungsfunktionen zulassen
- Für bestimmte Nutzer oder Gruppen zulassen

Mithilfe des Richtlinien-Editors, der ein vertrautes Aussehen und Verhalten aufweist, können erfahrene Firewalladministratoren schnell flexible Firewallrichtlinien wie die folgenden erstellen:

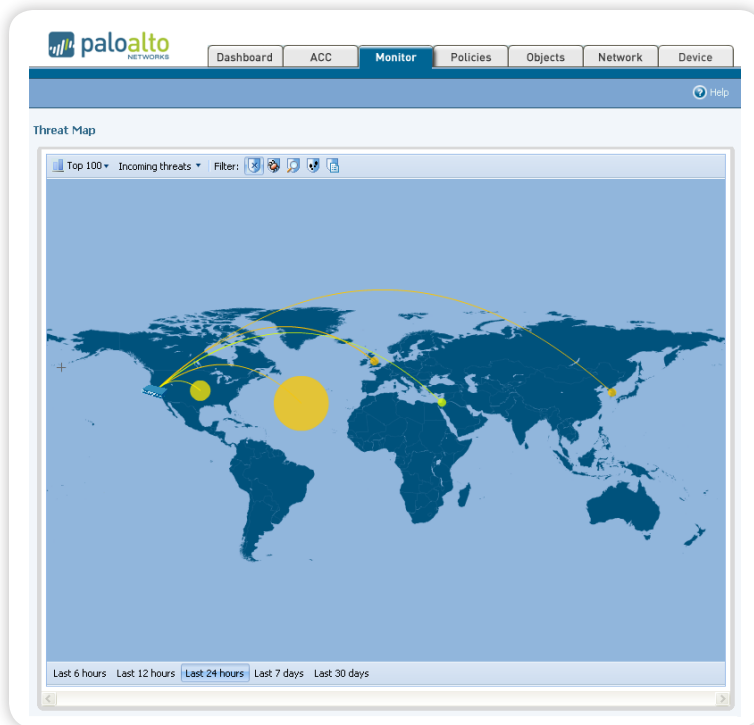
- Zuweisen von Salesforce.com und Oracle zu den Vertriebs- und Marketinggruppen durch Nutzung der Integration von Active Directory.
- Ausschließliches Zulassen der Verwendung einer festgelegten Palette von Managementanwendungen wie SSH, Telnet und RDP durch die IT-Gruppe.

- Malware wie P2P-Filesharing, Umgehungsprogramme und fremde Proxys blockieren.
- Festlegen und Erzwingen einer Unternehmensrichtlinie, die eine bestimmte Webmail- und Instant-Messaging-Nutzung zulässt und überprüft.
- Kontrolle der Dateiübertragungsfunktionalität in einzelnen Anwendungen, wobei die Verwendung der Anwendung zugelassen und gleichzeitig eine Dateiübertragung unterbunden werden können.
- Identifizieren der Übertragung von vertraulichen Informationen wie Kreditkartennummern, entweder im Text- oder Dateiformat.
- Implementierung 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“.
- Implementierung von Richtlinien zur Quality of Service, mit denen Media- und andere bandbreitenintensive Anwendungen unter Begrenzung ihrer Auswirkung auf geschäftskritische Anwendungen zugelassen werden.

Mit einer Firewall der nächsten Generation von Palo Alto Networks können Kunden Richtlinien für positive Erzwingungsmodelle implementieren, um Malware zu blockieren, die Geschäftsanwendungen zu schützen und die sichere Verwendung von Anwendungen für Endbenutzer zu fördern, was zu einem positiveren Arbeitsumfeld führt.

**Richtlinien-Editor**  
Ein vertrautes Aussehen und Verhalten gestattet die schnelle Entwicklung und Implementierung von Richtlinien, die Anwendungen, Benutzer und Inhalte kontrollieren.

Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1 No Intra-zone DMZ	DMZ	DMZ	any	any	any	any	any	none	none	
2 Do Not Traffic Log	tapzone	DMZ	any	any	any	LocalServers	any	none	none	
3 Do Not URL Log	tapzone	tapzone	any	any	any	LocalNetwork	ssl	none	none	
4 Monitor ALL	tapzone	tapzone	any	any	any	web-browsing	any	none	none	
5 Block P2P	any	untrust	any	any	any	P2P Filesharing	any	none	none	
6 Webmail - No Attachments	any	untrust	any	any	any	Webmail	any	none	none	
7 CEO YouTube	any	untrust	any	pancademojzielinski	any	youtube	any	none	none	
8 Block High Risk Media	any	untrust	any	any	any	High Risk Media	any	none	none	
9 Allow IT Remote Access	trust	untrust	any	pancademoadministrators	any	Remote Access	any	none	none	
10 CFO Warcraft	any	untrust	any	pancademojzsteller	any	worldofwarcraft	any	none	none	
11 Block Remote Access	any	untrust	any	any	any	Remote Access	any	none	none	
12 Control Finance Web Posting	trust	untrust	any	pancademo/finance	any	Web Posting	any	none	none	
13 General Web	any	untrust	any	any	any	web-browsing	any	none	none	
14 Inbound SMTP	untrust	DMZ	any	any	10.0.0.253	smtp	application-default	none	none	
15 Corp Webserver	untrust	DMZ	any	any	10.0.0.249	web-browsing	application-default	none	none	
16 Deny and Log Outbound	trust	untrust	any	any	any	any	any	none	none	
17 Deny and Log Inbound	untrust	trust	any	any	any	any	any	none	none	



#### Darstellung der Sicherheitsrisiken

Geografische Darstellung der Sicherheitsrisiken innerhalb und außerhalb des Netzwerks.

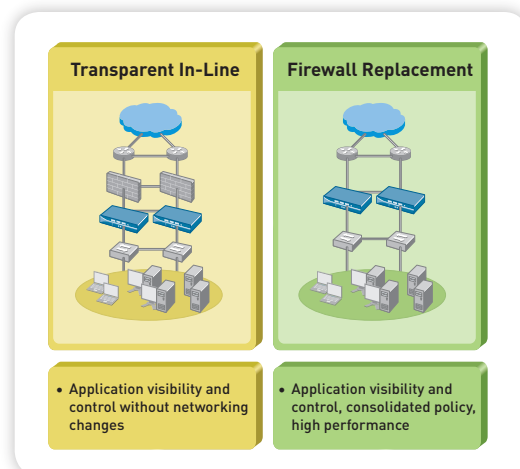
#### Identifizierung der Anwendung, Prüfung des Inhalts

Durch die präzise Identifikation und Kontrolle von Anwendungen mithilfe von App-ID können Anforderungen, die sich den IT-Abteilungen bezüglich Transparenz und Kontrolle 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.

- **Schutz vor Sicherheitsrisiken:** Bei dieser Komponente wird ein einheitliches Signaturformat mit Stream-basierter Überprüfung kombiniert, um gleichzeitig Viren, Spyware und Sicherheitslücken in Anwendungen in einem einzigen Durchlauf zu erkennen und zu blockieren. Der Schutz vor Sicherheitslücken in Anwendungen integriert eine Palette an Funktionen des Intrusion Prevention Systems (IPS, Schutz vor unbefugtem Zugriff), um bekannte und unbekannte Exploits für Sicherheitslücken im Netzwerk- und Anwendungslayer, Pufferüberläufe, Denial-of-Service-Attacken und Portüberprüfungen durch Ressourcen zu blockieren, die die Informationen des Unternehmens beeinträchtigen und schädigen. Zu den Mechanismen der Intrusion Prevention gehören:
  - Erkennung von Abweichungen von den gängigen Protokollen
  - Zustandsorientierter Musterabgleich
  - Erkennung von statistischen Abweichungen
  - Analyse auf heuristischer Basis
  - Blockieren unzulässiger oder missgestalteter Pakete
  - IP-Defragmentierung und TCP-Reassemblierung
- **URL-Filterung:** Eine vollständig integrierte anpassbare 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. Die URL-Datenbank kann erweitert werden, um mit den Datenverkehrsmustern der lokalen Nutzergemeinschaft übereinzustimmen. Falls ein URL entdeckt wird, der nicht in der lokalen URL-Datenbank kategorisiert ist, kann die Firewall die Kategorie von einer gehosteten URL-Datenbank anfordern, die über 180 Millionen URLs enthält. Der URL wird dann lokal in einer separaten dynamischen URL-Datenbank mit 1 Million Einträgen gespeichert.
- **Datei- und Datenfilterung:** Indem das Content-ID-Modul die umfassende Analyse durch App-ID in vollem Umfang ausschöpft, versetzt es Administratoren in die Lage, Richtlinien für die Filterung von Daten zu implementieren. Dadurch werden die Risiken einer nicht autorisierten Datenübertragung minimiert. Dateien in Abhängigkeit von ihrem Typ (anstatt dazu lediglich die Dateierweiterung zu nutzen) und Muster vertraulicher Daten (Kreditkarten) können anhand der Richtlinie erkannt und blockiert werden.

**Optionen für die flexible Bereitstellung**

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

**Netzwerk**

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

- **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.
- **IPv6:** Es werden vollständige Anwendungstransparenz, Kontrolle, Filterung, Überwachung und Protokollierung für Anwendungen, die IPv6 verwenden, unterstützt (nur im Virtual-Wire-Modus).
- **Switching und Routing:** Die Unterstützung des L2-, L3- und des gemischten Modus in Kombination mit zonenbasierter Sicherheit ermöglicht die Implementierung in zahlreiche Netzwerkumgebungen. Dynamische Routingprotokolle (OSPF und RIP) und umfassende 802.1Q VLAN-Unterstützung werden sowohl für L2 als auch L3 bereitgestellt
- **Aktive/passive hohe Verfügbarkeit:** Hardwareredundanz mit voller Unterstützung für Konfigurations- und Sitzungssynchronisierung.
- **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.
- **Fernzugriff VPN:** Der SSL Tunnel VPN gewährleistet einen sicheren Netzwerkzugriff durch Remotebenutzer und erweitert die richtlinienbasierte Transparenz und Kontrolle über Anwendungen, Benutzer und Inhalte für diese Benutzer.

- **Quality of Service (QoS):** Die Optimierung der Kapazitätsauslastung erweitert die Kontrollen der Richtlinie zur positiven Tauglichkeit und gibt Administratoren damit die Möglichkeit, bandbreitenintensive Anwendungen wie Streaming Media zuzulassen und gleichzeitig die Leistungsfähigkeit der Geschäftsanwendungen zu erhalten. Richtlinien zur Optimierung der Kapazitätsauslastung (garantiert, maximal und vordringlich) können nach Anwendung, Benutzer, Zeitplan und anderem erzwungen werden. DiffServ-Markierung wird ebenso unterstützt, sodass der Anwendungsverkehr mithilfe eines nach- oder vorgeschalteten Geräts kontrolliert werden kann.

**Berichterstellung und Protokollierung:**

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

- **Berichterstellung:** Vordefinierte Berichte können im Ist-Zustand verwendet, angepasst oder miteinander zu einem Report gruppiert werden, um den spezifischen Anforderungen zu entsprechen. Ein detaillierter Aktivitätenbericht zeigt die verwendeten Anwendungen, die besuchten URL-Kategorien, die besuchten Websites und einen detaillierten Bericht über alle URLs, die von einem gegebenen Benutzer über einen bestimmten Zeitraum hinweg besucht wurden. Alle Berichte können ins CSV- oder PDF-Format exportiert und nach Zeitplan per E-Mail gesendet werden.
- **Protokollierung:** Administratoren können Aktivitäten im Zusammenhang mit Anwendungen, Sicherheitsrisiken und Benutzern mithilfe von dynamischen Filterfunktionen anzeigen, die einfach aktiviert werden können, indem Sie auf einen Wert in einer Zelle klicken und/oder die Filterkriterien mithilfe des Ausdrucks-Generators festlegen. Protokollfilterergebnisse können zur Offline-Archivierung oder zur zusätzlichen Analyse in eine CSV-Datei exportiert oder an einen Syslog-Server gesendet werden.