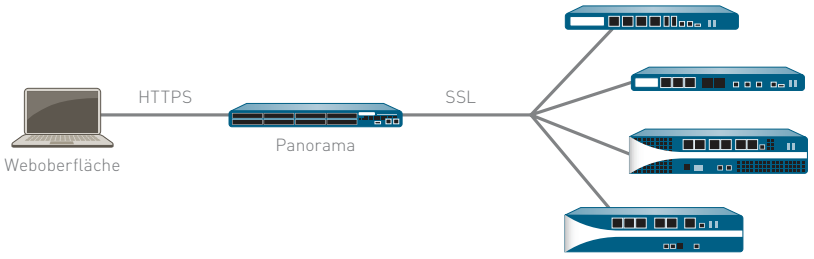
PANORAMA

Panorama bietet eine zentralisierte Richtlinien- und Geräteverwaltung über ein Netzwerk aus Palo Alto Networks-Firewalls der nächsten Generation.

- Zeigen Sie eine grafische Zusammenfassung der Anwendungen des Netzwerks, der entsprechenden Benutzer und der potenziellen Auswirkungen auf die Sicherheit an.
- Stellen Sie Unternehmensrichtlinien zentral bereit, damit bei der Nutzung in Zusammenhang mit lokalen Richtlinien maximale Flexibilität entsteht.
- Schaffen Sie geeignete administrative Kontrollstufen auf Geräteebene oder global mit rollenbasiertem Management.
- Netzwerkverkehr, Sicherheitsvorfälle und administrative Änderungen können zentral analysiert, geprüft und gemeldet werden.



Große Unternehmen haben in der Regel zahlreiche Firewalls in ihr Netzwerk integriert, wodurch die Verwaltung und Steuerung aufgrund der Komplexität und Uneinheitlichkeit zwischen den einzelnen Geräten häufig erschwert wird. Dadurch entstehen ein höherer Verwaltungsaufwand und zusätzliche damit verbundene Kosten.

Panorama bietet eine zentralisierte Verwaltung und Transparenz der Palo Alto Networks-Firewalls der nächsten Generation. Administratoren erhalten von einem zentralen Standort aus Einblick in die Anwendungen, Benutzer und Inhalte, die sich durch die Firewalls bewegen. Mit dem Wissen, was sich im Netzwerk befindet, und den Richtlinien für die Zulassung von Anwendungen lassen sich der Schutz und die Kontrolle maximieren, während der Verwaltungsaufwand gleichzeitig verringert wird. Administratoren können mit den Aggregatdaten oder den auf der lokalen Firewall gespeicherten Daten zentral und im Zeitverlauf Analysen und Berichte erstellen und forensische Untersuchungen vornehmen.

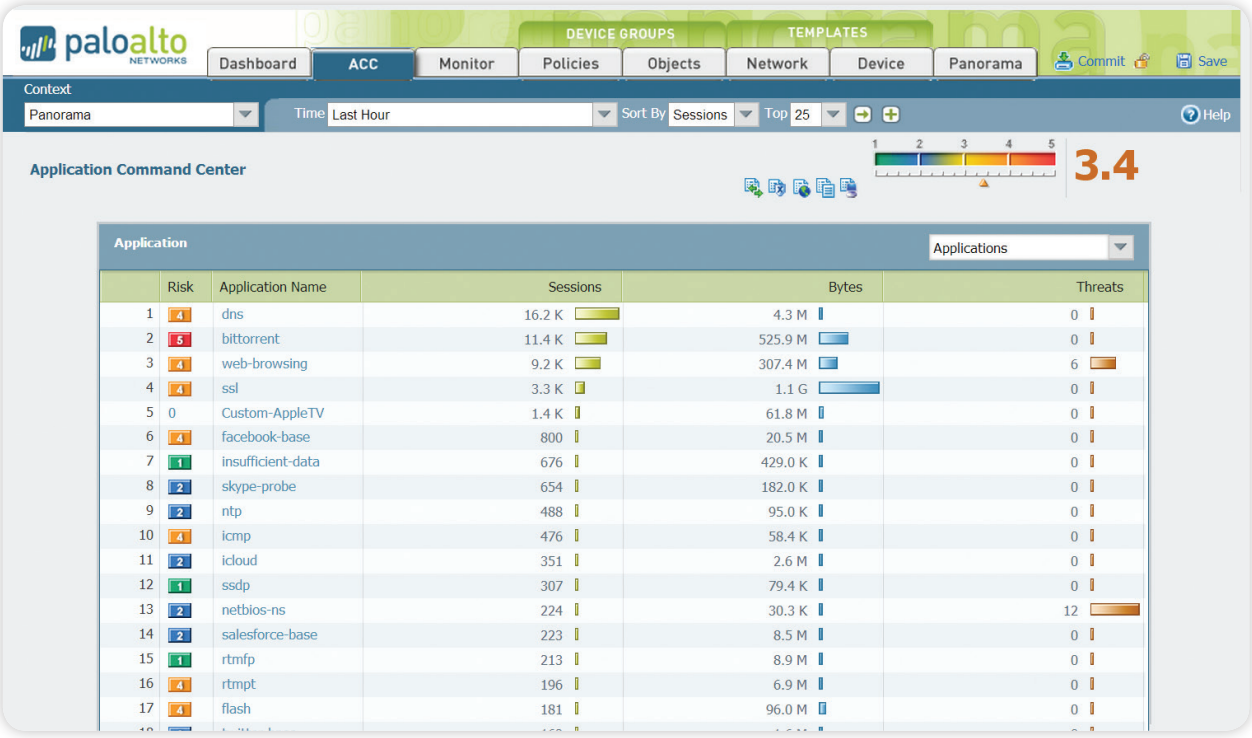
Panorama und die einzelnen Geräte verfügen über das gleiche webbasierte Aussehen und Verhalten, wodurch die Lernkurve nicht sehr steil ist und die anfallenden Aufgaben ohne Verzögerung ausgeführt werden können. Palo Alto Networks befolgt eine Verwaltungsphilosophie mit Schwerpunkt auf Konsistenz, was dem Unternehmen einen enormen Fortschritt gegenüber der Konkurrenz verschafft.

Zentrale Transparenz: Application Command Center

Application Command and Control (ACC) von Panorama zeigt den Administratoren eine grafische Übersicht über die Anwendung, URL, Bedrohung und Daten (Dateien und Muster) in den verwalteten Palo Alto Networks-Geräten. ACC ruft dynamisch Daten von jedem Gerät ab. So haben Administratoren stets einen aktuellen Überblick über die Anwendungen im Netzwerk, wissen, wer sie verwendet und kennen die Bedrohungen, die möglicherweise von ihnen ausgehen. Administratoren können neue oder unbekannte Anwendungen mit nur einem Klick untersuchen. Auf diese Weise werden eine Beschreibung der Anwendung, ihre wichtigsten Funktionen, ihre Verhaltenseigenschaften und ihre Benutzer angezeigt.

Zusätzliche Daten zu URL-Kategorien und Bedrohungen bieten ein vollständiges und abgerundetes Bild der Netzwerkaktivität. Dank der Transparenz von ACC können Administratoren fundierte Richtlinienentscheidungen treffen und schnell auf potenzielle Sicherheitsbedrohungen reagieren.

paloalto NETWORKS
the network security company™



Application Command Center bietet globale und lokale Ansichten des Anwendungsverkehrs einschließlich Drilldown, wodurch Sie mehr über die aktuelle Aktivität erfahren können.

Globale Richtlinienkontrolle: Sichere Anwendungsaktivierung

Die sichere Aktivierung von Anwendungen bedeutet, dass mit speziellen Richtlinien für den Schutz vor Bedrohungen und der Blockierung von Dateien oder zur URL-Filterung Zugriff auf bestimmte Anwendungen gestattet wird. Panorama ermöglicht eine sichere Anwendungsaktivierung im gesamten Netzwerk der Firewalls, indem Administratoren Regeln von einem zentralen Standort aus verwalten können.

Mithilfe von Panorama-basierten gemeinsamen Richtlinien wird die Einhaltung von internen oder rechtlichen Anforderungen gewährleistet, während die Sicherheit und Flexibilität durch die Regeln der lokalen Geräte beibehalten wird. Durch die Kombination von zentralisierter und lokaler administrativer Kontrolle der Richtlinien und Objekte kann eine konsistente Sicherheit auf globaler und Flexibilität auf lokaler Ebene erreicht werden.

Administratoren können Richtlinien implementieren, durch die Anwendungen oder Anwendungsfunktionen basierend auf den Benutzern sicher aktiviert werden. Dies erfolgt über eine Integration der Verzeichnisdienste. Gleichzeitig werden die Inhalte und das Netzwerk durch einen anwendungsspezifischen Bedrohungsschutz geschützt. Durch die Möglichkeit, eine einzelne Richtlinie festzulegen, die die sichere Aktivierung der Anwendungen basierend auf dem Benutzer und nicht auf der IP-Adresse gestattet, können Unternehmen die Anzahl der erforderlichen Richtlinien enorm reduzieren. Ein weiterer Vorteil der Integration der Verzeichnisdienste ist eine Senkung der Verwaltungskosten, die durch Neueinstellungen oder Stellenwechsel im Unternehmen entstehen – die Sicherheitsrichtlinien bleiben immer gleich, auch wenn Mitarbeiter von einer Gruppe in eine andere wechseln.

Verkehrsüberwachung: Analyse, Reporting und Forensik

Panorama verwendet den gleichen Satz an leistungsstarken Überwachungs- und Reporting-Tools, die auch für die lokale Geräteverwaltung verfügbar sind. Eine Aggregatansicht der Aktivitäten bietet zusätzliche Transparenz. Wenn Administratoren Anfragen protokollieren und Berichte erstellen, ruft Panorama dynamisch die aktuellen Daten direkt von den verwalteten Firewalls oder aus Protokollen, die an Panorama weitergeleitet wurden, ab. Dadurch, dass Administratoren auf allen Geräten auf die neusten Informationen zugreifen können, lassen sich Sicherheitsvorfälle schneller beheben und das Firmenvermögen kann proaktiv geschützt werden.

- **Protokollanzeige:** Panorama-Administratoren können unmittelbar Protokollaktivitäten für einzelne oder alle Geräte mithilfe einer dynamischen Protokollfilterung anzeigen. Dies funktioniert durch Klicken auf einen Zellwert und/oder über ein Tool zur Erstellung von Ausdrücken, mit dem sich die Sortierungskriterien definieren lassen. Die Ergebnisse können für zukünftige Anfragen gespeichert oder für weitere Analysen exportiert werden.
- **Benutzerdefiniertes Reporting:** Vordefinierte Berichte können im Ist-Zustand verwendet, angepasst oder miteinander zu einem Report gruppiert werden, um den spezifischen Anforderungen zu entsprechen.
- **Berichte zur Benutzeraktivität:** Ein von Panorama erstellter Bericht zur Benutzeraktivität zeigt die verwendeten Anwendungen, besuchten URL-Kategorien und Webseiten sowie alle besuchten URLs über einen bestimmten Zeitraum für einzelne Benutzer. Panorama generiert den Bericht mithilfe einer Aggregatansicht der Benutzeraktivität, unabhängig davon, von welcher Firewall sie geschützt wird oder welche IP bzw. welches Gerät benutzt wurde.

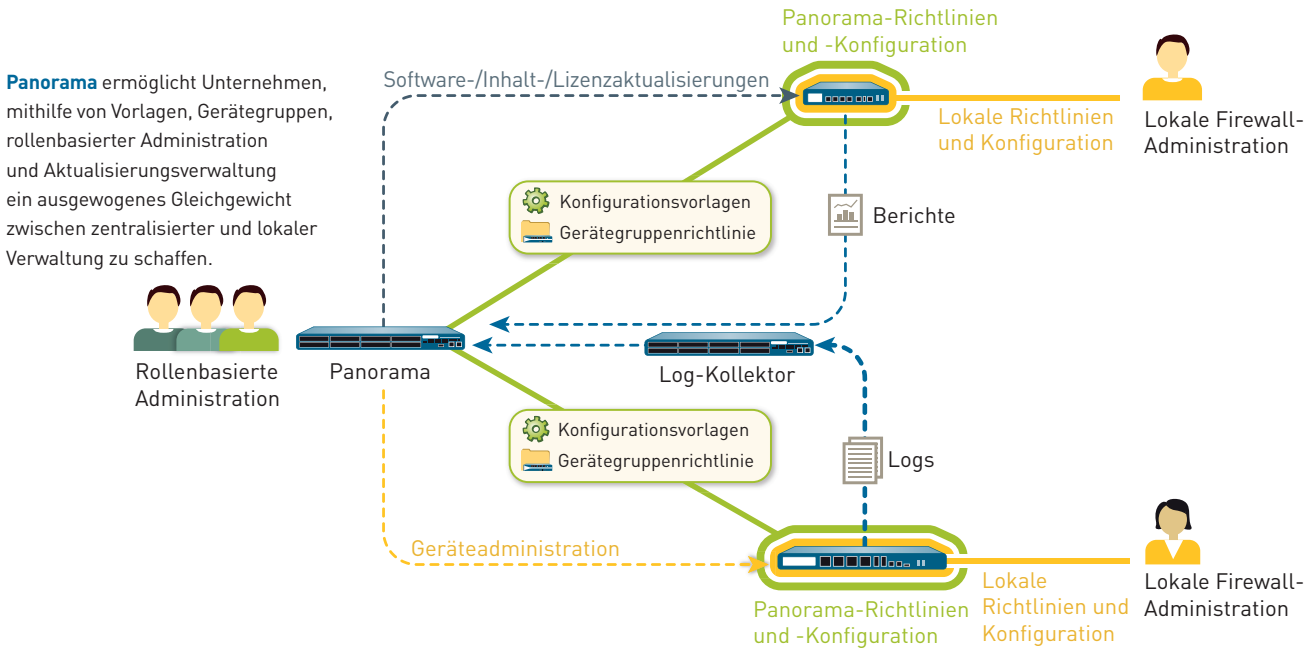
Panorama-Verwaltungsarchitektur

Panorama ermöglicht Unternehmen, ihre Palo Alto Networks-Firewalls mithilfe eines Modells zu verwalten, das sowohl zentralen Überblick als auch lokale Kontrolle bietet. Panorama stellt eine Reihe von Tools für die zentralisierte Administration zur Verfügung:

- **Vorlagen:** Panorama verwaltet die allgemeine Geräte- und Netzwerkkonfiguration über Vorlagen. Vorlagen können zur zentralen Konfiguration verwendet werden. Die Änderungen werden dann an alle verwalteten Firewalls gepusht. Durch diese Lösung wird vermieden, dass einzelne Änderungen an der Firewall für mehrere Geräte wiederholt werden müssen. Beispielsweise können allgemeine DNS- und NTP-Servereinstellungen über Hunderte Firewalls hinweg gepusht werden, ohne dass die gleiche Änderung Gerät für Gerät vorgenommen werden muss.
- **Gerätegruppe:** Panorama verwaltet allgemeine Richtlinien und Objekte durch Gerätegruppen. Gerätegruppen werden verwendet, um die Regelwerke zahlreicher Geräte mit allgemeinen Anforderungen zu verwalten. Die Geräte können beispielsweise in geografische (z. B. Europa oder Nordamerika) oder funktionsorientierte (z. B. Perimeter oder Rechenzentrum) Gerätegruppen eingeordnet werden. Innerhalb der Gerätegruppen werden virtuelle Systeme als individuelle Geräte betrachtet, die sich auf derselben Ebene befinden wie physische Firewalls. Dadurch können allgemeine Regelwerke für verschiedene virtuelle Systeme auf einem Gerät freigegeben werden.

  Unternehmen können gemeinsame Richtlinien für die zentrale Kontrolle verwenden. Der Firewall-Administrator hat jedoch weiterhin die Möglichkeit, bestimmte Anpassungen für lokale Anforderungen vorzunehmen. Auf Gerätegruppenebene können Administratoren gemeinsame Richtlinien erstellen, die als erster („Pre-Rules“) und letzter Regelsatz („Post-Rules“) definiert werden. Diese können anhand der Übereinstimmungskriterien bewertet werden. Pre- und Post-Rules können auf einer verwalteten Firewall angezeigt werden, die Bearbeitung ist jedoch nur über Panorama im Rahmen von definierten administrativen Rollen möglich. Lokale Geräteregeln (zwischen Pre- und Post-Rules) können vom lokalen Administrator oder einem auf Ebene der lokalen Firewall zugeschalteten Panorama-Administrator bearbeitet werden. Weiterhin können Unternehmen gemeinsame Objekte verwenden, die von einem Panorama-Administrator definiert wurden und auf die durch lokal verwaltete Geräteregeln verwiesen werden kann.
- **Rollenbasierte Administration:** Unternehmen können eine rollenbasierte Administration nutzen, um administrativen Zugang auf Funktionsebene (aktiviert, schreibgeschützt, deaktiviert oder ausgeblendet) für verschiedene Mitarbeiter zu ermöglichen. Bestimmte Administratoren können entsprechenden Zugriff auf die Aufgaben erhalten, für die sie verantwortlich sind, während andere Zugriffe ausgeblendet oder schreibgeschützt sind. Mit dieser Art von Zugriffskontrolle können beispielsweise verschiedene Rollen für Mitarbeiter definiert werden, die für verschiedene Aufgaben im Unternehmen verantwortlich sind (Sicherheitsadministratoren im Vergleich zu Netzwerkadministratoren). Sämtliche von einem Administrator vorgenommene Änderungen werden protokolliert. Dabei werden die Uhrzeit, der Administrator, die verwendete Verwaltungsschnittstelle (Web UI, CLI, Panorama), der Befehl und die durchgeführte Aktion aufgezeichnet.
- **Verwaltung von Software, Inhalt und Lizenzaktualisierung:** Mit wachsenden Implementierungen möchten die Unternehmen sicherstellen, dass Aktualisierungen in organisierter Art und Weise an verteilte Geräte ausgerollt werden. Sicherheitsteams möchten eine Software-Aktualisierung möglicherweise erst zentral qualifizieren, bevor sie über Panorama gleichzeitig an alle Produktions-Firewalls verteilt wird. Mithilfe von Panorama kann der Aktualisierungsvorgang für Software-Aktualisierungen, Inhalt (Anwendungsaktualisierungen, Virenschutzsignaturen, Bedrohungssignaturen, URL-Filterdatenbank usw.) und Lizenzen zentral verwaltet werden.

Unter Verwendung von Vorlagen, Gerätegruppen, rollenbasierter Administration und Aktualisierungsverwaltung können Unternehmen allen Verwaltungsfunktionen entsprechenden Zugriff gewähren – Visualisierungs-Tools, Richtlinienerstellung, Reporting und Protokollierung auf globaler und lokaler Ebene.



Flexibilität bei der Bereitstellung

Panorama kann entweder als Hardware- oder als virtuelle Anwendung implementiert werden.

Hardware Appliance

Für Unternehmen, die eine Bereitstellung in Form von leistungsstarker Hardware bevorzugen oder die Panorama-Verwaltung und die Protokollierungsfunktionen für große Mengen an Protokolldaten voneinander trennen möchten, ist die Hardware Appliance M-100 die richtige Wahl. Es gibt folgende Möglichkeiten zur Bereitstellung von Panorama auf dem Modell M-100:

- **Zentralisiert:** In diesem Fall werden sämtliche Verwaltungs- und Protokollierungsfunktionen von Panorama auf einem einzelnen Gerät zusammengeführt (mit optionaler Hochverfügbarkeit).
- **Verteilt:** Einige Unternehmen bevorzugen eine Aufteilung der Verwaltungs- und Protokollierungsfunktionen auf mehrere Geräte. Bei dieser Konfiguration werden die Funktionen zwischen Managern und Log-Kollektoren aufgeteilt.
  - **Panorama-Manager:** Der Panorama-Manager bearbeitet die Aufgaben in Zusammenhang mit der Richtlinien- und Gerätekonfiguration in allen verwalteten Geräten. Der Manager speichert Protokolldaten nicht lokal, sondern verwendet separate Log-Kollektoren für die Bearbeitung von Protokolldaten. Der Manager analysiert die in den Log-Kollektoren gespeicherten Daten für zentralisiertes Reporting.
  - **Panorama-Log-Kollektor:** Unternehmen mit großem Protokollierungsvolumen und Aufbewahrungsanforderungen können entsprechende Log-Kollektor-Geräte von Panorama implementieren, die Protokollinformationen von verschiedenen verwalteten Firewalls sammeln.

Durch die Trennung von Verwaltungsfunktionen und Protokollsammlung können Unternehmen ihre Bereitstellung optimieren, um die organisatorischen und geografischen sowie die Anforderungen an die Skalierbarkeit zu erfüllen.

Virtuelle Appliance

Panorama kann auch als virtuelle Appliance auf VMware ESX(i) bereitgestellt werden, was den Unternehmen ermöglicht, ihre Virtualisierungsinitiativen zu unterstützen und Rack-Platz zu sparen, der in einem Rechenzentrum häufig beschränkt oder teuer ist. Bei der Bereitstellung der virtuellen Anwendung gibt es zwei Möglichkeiten:

- **Zentralisiert:** Sämtliche Verwaltungs- und Protokollierungsfunktionen von Panorama sind auf einer einzelnen virtuellen Anwendung zusammengeführt (mit optionaler Hochverfügbarkeit).
- **Verteilt:** Die verteilte Protokollsammlung von Panorama unterstützt eine Mischung aus Hardware und virtueller Appliance.
  - **Panorama-Manager:** Die virtuelle Anwendung kann als Panorama-Manager dienen. Über sie werden die Aufgaben im Zusammenhang mit der Richtlinien- und Gerätekonfiguration in allen verwalteten Geräten bearbeitet.
  - **Panorama-Log-Kollektor:** Die Panorama-Log-Kollektoren sind für die Entlastung bei intensiven Protokollsammlungs- und Verarbeitungsaufgaben zuständig und können über die Hardware Appliance M-100 implementiert werden. Die virtuelle Appliance kann nicht als Panorama-Log-Kollektor verwendet werden.

Die Wahl zwischen Hardware- oder virtualisierter Plattform und zwischen Kombination oder Trennung der Panorama-Funktionen bietet den Unternehmen maximale Flexibilität bei der Verwaltung mehrerer Palo Alto Networks-Firewalls in einer verteilten Netzwerkumgebung.

PANORAMA-SPEZIFIKATIONEN

Anzahl der unterstützten Geräte	Bis zu 1.000
Hohe Verfügbarkeit	Aktiv/Passiv
Administrator-Authentifizierung	Lokale Datenbank
	RADIUS

SPEZIFIKATIONEN DER M-100-VERWALTUNGSANWENDUNG

E/A

- (1) 10/100/1000, (3) 10/100/1000 (für zukünftige Nutzung), (1) serieller Konsolenport DB9

SPEICHER (2 OPTIONEN)

- M-100 1 TB RAID: 2 x 1 TB RAID-zertifizierte HDD für 1 TB RAID-Speicher
- M-100 4 TB RAID: 8 x 1 TB RAID-zertifizierte HDD für 4 TB RAID-Speicher

STROMZUFUHR/MAX. STROMVERBRAUCH

- 500 W/500 W

MAX. BTU/H

- 1.705 BTU/h

EINGANGSSPANNUNG (EINGANGSFREQUENZ)

- 100–240 VAC (50–60 Hz)

MAX. STROMVERBRAUCH

- 10 A @ 100 VAC

MEAN TIME BETWEEN FAILURE (MTBF)

14,5 Jahre

IM RACK MONTIERBAR (ABMESSUNGEN)

- 1 Einheit, 48,26 cm-Standard-Rack (2,54 cm H x 58,42 cm T x 43,67 cm B)

GEWICHT (STAND-ALONE-GERÄT/WIE GELIEFERT)

- 12,1 kg/n.n. kg

SICHERHEIT

- UL, CUL, CB

EMI

- FCC-Klasse A, CE-Klasse A, VCCI-Klasse A

UMGEBUNG

- Betriebstemperatur: 5 bis 40 °C
- Temperatur bei Nichtbetrieb: -40 bis 65 °C

SPEZIFIKATIONEN DER VIRTUELLEN ANWENDUNG

MINDEST-SERVER-ANFORDERUNGEN

- 40 GB Festplatte
- 4 GB RAM
- Quad-Core CPU (2GHz+)

VMWARE-SUPPORT

- VMware ESX 4.1 oder höher

BROWSER-SUPPORT

- IE v7 oder höher
- Firefox v3.6 oder höher
- Safari v5.0 oder höher
- Chrome v11.0 oder höher

PROTOKOLLSPEICHER

- VMware Virtual Disk: Max. 2 TB
- NFS

paloalto NETWORKS
the network security company™

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