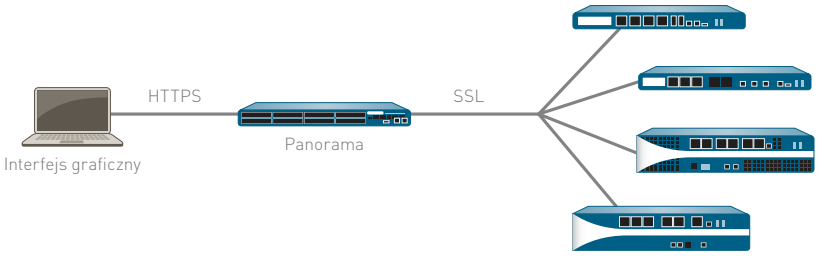
PANORAMA

System Panorama umożliwia centralne zarządzanie politykami i urządzeniami w sieciach, w których zastosowano najnowsze zapory firmy Palo Alto Networks.

- Wyświetlanie graficznego podsumowania aplikacji w sieci, odpowiednich użytkowników oraz potencjalnego wpływu na bezpieczeństwo.
- Centralne wdrażanie polityk korporacyjnych do stosowania razem z politykami lokalnymi w celu zapewnienia maksymalnej elastyczności.
- Delegowanie odpowiednich poziomów kontroli administracyjnej na poziomie urządzeń lub globalnie w ramach zarządzania opartego na rolach.
- Scentralizowane analizowanie, badanie i raportowanie ruchu sieciowego, incydentów związanych z bezpieczeństwem oraz modyfikacji administracyjnych.



W sieciach dużych organizacji wdrożonych jest zwykle wiele zapór, a proces zarządzania nimi oraz ich kontroli jest najczęściej utrudniony ze względu na złożoność i niezgodności pomiędzy poszczególnymi urządzeniami. Skutkiem takiej sytuacji jest zwiększenie liczby zadań administracyjnych oraz związanych z nimi kosztów.

System Panorama umożliwia centralne zarządzanie i wgląd w informacje o zaporach nowej generacji firmy Palo Alto Networks. Z jednej centralnej lokalizacji administratorzy mogą monitorować aplikacje, użytkowników i zawartość przechodzącą przez zapory. Wiedza o kondycji sieci w połączeniu z politykami zapewniającymi bezpieczne korzystanie z aplikacji gwarantuje maksymalną ochronę i kontrolę przy minimalnym zakresie czynności administracyjnych. Administratorzy mogą wykonywać w centralnej lokalizacji analizy, raporty i badania na danych zgromadzonych w wybranym okresie lub danych zapisanych w zaporze lokalnej.

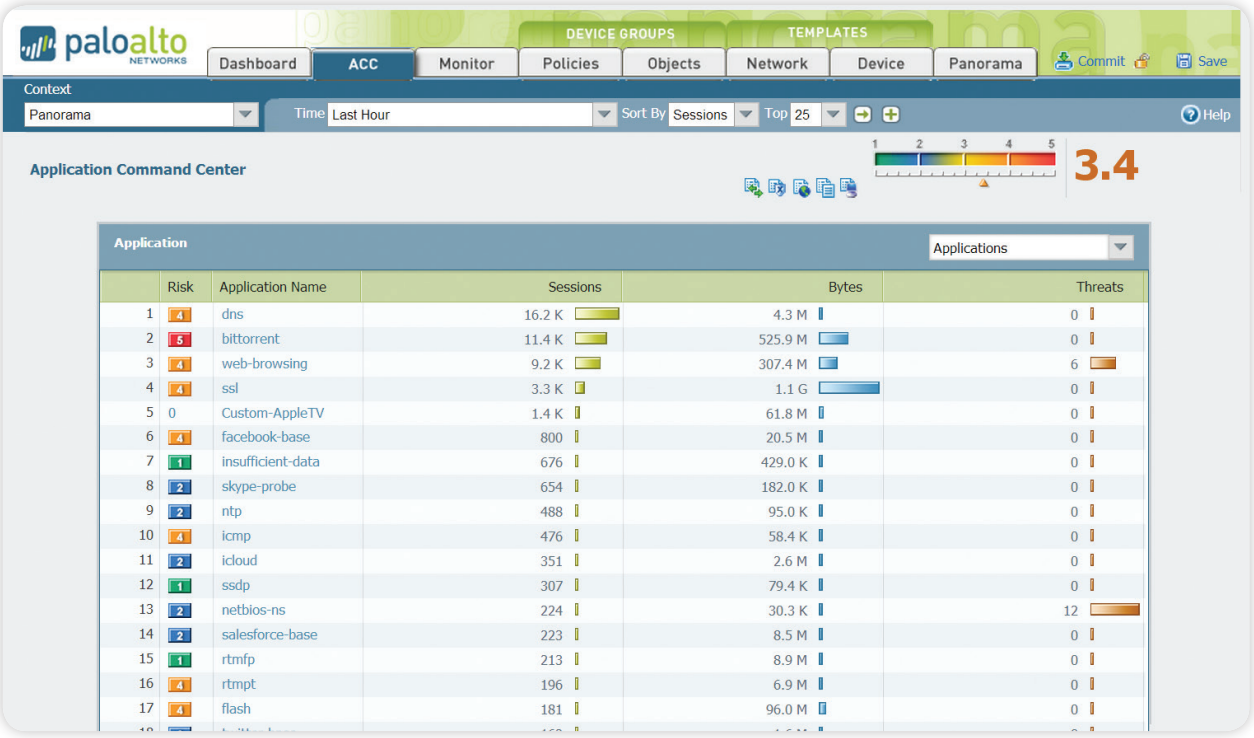
Zarówno system Panorama, jak i poszczególne urządzenia korzystają z identycznego interfejsu graficznego, co skraca czas nauki obsługi i eliminuje opóźnienia w wykonywaniu zadań. Firma Palo Alto Networks dba o zgodność z filozofią zarządzania, która kładzie nacisk na spójność, zapewniając znaczną przewagę konkurencyjną nad innymi dostępnymi na rynku rozwiązaniami.

Scentralizowany wgląd w informacje o sieci: Application Command Center

Dostępna w systemie Panorama funkcja ACC (Application Command Center) udostępnia administratorowi graficzny podgląd aplikacji, adresów URL, zagrożeń i danych (plików i wzorców) przechodzących przez zarządzane urządzenia firmy Palo Alto Networks. Funkcja ACC dynamicznie pobiera dane z poszczególnych urządzeń, zapewniając administratorom dostęp do aktualnego widoku parametrów aplikacji w sieci, użytkowników korzystających z tych aplikacji oraz potencjalnych zagrożeń, które mogą wystąpić. Administratorzy mogą w ten sposób badać nowe lub nieznane aplikacje. Jednym kliknięciem można wyświetlić opis aplikacji, jej główne cechy, charakterystykę jej zachowań oraz użytkowników korzystających z tej aplikacji.

Dodatkowe dane na temat kategorii adresów URL oraz zagrożeń uzupełniają obraz aktywności sieciowej. Podgląd parametrów za pośrednictwem funkcji ACC pozwala administratorom podejmować przemyślane decyzje i szybko reagować na potencjalne zagrożenia bezpieczeństwa.

paloalto NETWORKS
the network security company™



Funkcja Application Command Center udostępnia globalne i lokalne widoki ruchu sieciowego w aplikacjach, uzupełnione szczegółowymi informacjami na temat bieżącej aktywności sieciowej.

Globalna kontrola polityk: bezpieczne korzystanie z aplikacji

Bezpieczne korzystanie z aplikacji oznacza możliwość dostępu do określonych aplikacji z zastosowaniem określonych zabezpieczeń przed zagrożeniami oraz polityk filtrowania plików, danych lub adresów URL. System Panorama zapewnia bezpieczne korzystanie z aplikacji w całej sieci z zaporami, umożliwiając administratorom zarządzanie politykami z jednej centralnej lokalizacji.

Współużytkowane polityki systemu Panorama pomagają w zapewnianiu zgodności z wewnętrznymi lub krajowymi przepisami, natomiast lokalne polityki urządzeń odpowiadają za zapewnianie bezpieczeństwa i elastyczności obsługi. Dzięki połączeniu centralnej i lokalnej kontroli administracyjnej polityk i obiektów można uzyskać równowagę między stałym bezpieczeństwem na poziomie globalnym a elastycznością na poziomie lokalnym.

Administratorzy mogą wdrażać polityki i zapewniać bezpieczną obsługę aplikacji lub ich funkcji według użytkowników za pośrednictwem mechanizmu integracji z usługami katalogowymi, natomiast zabezpieczenia aplikacji przed zagrożeniami chronią zawartość i sieć. Dzięki możliwości skonfigurowania pojedynczych polityk zapewniających bezpieczną obsługę aplikacji według użytkowników, a nie adresów IP, organizacje mogą znacznie ograniczyć liczbę wymaganych polityk. Dodatkową zaletą mechanizmu integracji z usługami katalogowymi jest znaczne zmniejszenie liczby zadań administracyjnych związanych z dodawaniem i przenoszeniem pracowników, a także zmianami występującymi w codziennej pracy, ponieważ polityki zabezpieczeń pozostają bez zmian podczas przenoszenia pracowników między grupami.

Monitorowanie ruchu: analizy, raporty i badania

System Panorama korzysta z tego samego zestawu narzędzi do monitorowania i tworzenia raportów, co narzędzia dostępne na lokalnym poziomie zarządzania urządzeniami oraz zapewnia podgląd parametrów w zbiorczym widoku aktywności w sieci. Podczas przesyłania przez administratorów zapytań dziennika oraz generowania raportów system Panorama dynamicznie pobiera najbardziej aktualne dane bezpośrednio z zarządzanych zapór lub dzienników przekazywanych do systemu Panorama. Dostęp do najnowszych informacji ze wszystkich urządzeń umożliwia administratorom reagowanie na incydenty związane z bezpieczeństwem oraz podejmowanie aktywnych działań zapobiegawczych w celu ochrony zasobów organizacji.

- **Podgląd dziennika:** W systemie Panorama administratorzy mogą szybko wyświetlić za pomocą funkcji dynamicznego filtrowania dziennika zarejestrowane aktywności dotyczące wybranych lub wszystkich urządzeń, klikając wartość w wybranej komórce i/lub definiując kryteria sortowania za pomocą edytora wyrażeń. Wyniki można zapisać do późniejszego użycia lub wyeksportować do dalszej analizy.
- **Raporty niestandardowe:** Wstępnie zdefiniowanych raportów można użyć w postaci niezmienionej, niestandardowej lub pogrupowanej w formie jednego raportu, w zależności od potrzeb.
- **Raporty dotyczące aktywności użytkowników:** Raport aktywności użytkowników w systemie Panorama zawiera używane aplikacje, kategorie odwiedzonych adresów URL, odwiedzone witryny internetowe oraz wszystkie adresy URL odwiedzone w wybranym okresie przez poszczególnych użytkowników. System Panorama tworzy raporty przy użyciu zbiorczego widoku aktywności użytkowników, niezależnie od tego, przez którą zaporę są chronieni lub którego adresu IP bądź urządzenia używają.

Architektura zarządzania w systemie Panorama

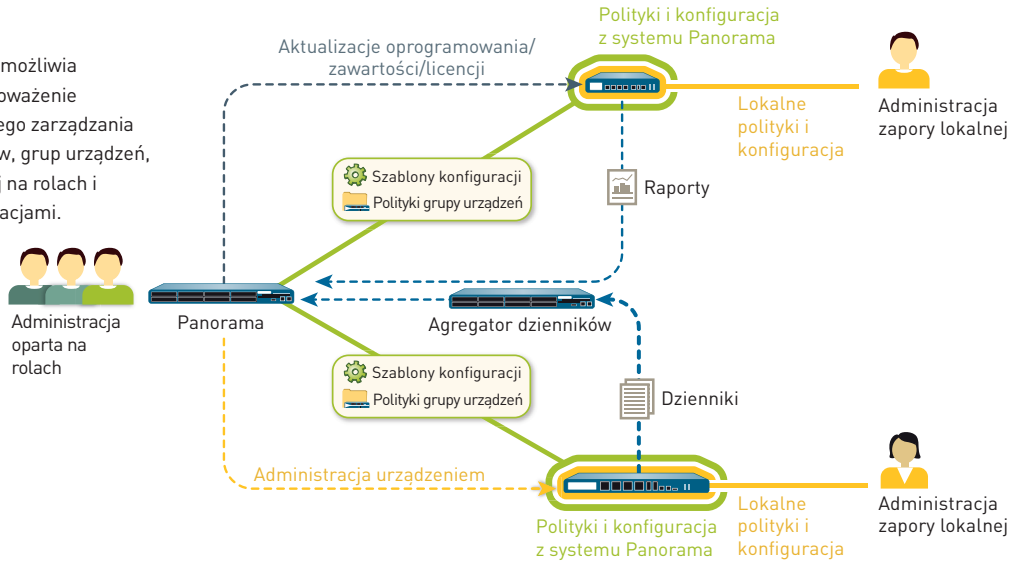
System Panorama umożliwia organizacjom zarządzanie zaporami firmy Palo Alto Networks z zastosowaniem modelu łączącego centralny nadzór z lokalną kontrolą. System Panorama udostępnia szereg narzędzi do centralnego administrowania:

- **Szablony:** System Panorama zarządza wspólną konfiguracją urządzeń i sieci za pomocą szablonów. Korzystając z szablonów, można zarządzać konfiguracją centralnie, a następnie rozesłać zmiany do wszystkich zarządzanych zapór. Metoda ta eliminuje konieczność wprowadzania osobnych zmian w zaporach na wielu urządzeniach. Przykładem takiego zastosowania jest rozsyłanie wspólnych ustawień serwera DNS i NTP do wielu zapór zamiast wprowadzania identycznej zmiany na każdym urządzeniu.
- **Grupy urządzeń:** System Panorama zarządza wspólnymi politykami i obiektami za pomocą grup urządzeń. Grupy urządzeń służą do centralnego zarządzania bazami polityk wielu urządzeń o wspólnych wymaganiach. Przykładami grup urządzeń mogą być grupy geograficzne (np. Europa i Ameryka Północna) lub funkcjonalne (np. sieć brzegowa lub centrum danych). Systemy wirtualne są traktowane w ramach grup urządzeń jako osobne urządzenia na równi z zaporami fizycznymi. Umożliwia to stosowanie wspólnej bazy polityk dla różnych systemów wirtualnych w urządzeniu.

  Organizacje mogą używać współużytkowanych polityk do centralnej kontroli, zapewniając jednocześnie administratorowi zapory autonomię we wprowadzaniu zmian w wymaganiach lokalnych. Na poziomie grupy urządzeń administratorzy mogą tworzyć współużytkowane polityki, które są definiowane jako pierwszy (reguły wstępne) oraz ostatni zestaw reguł (reguły końcowe) do sprawdzenia pod względem zgodności z kryteriami. Reguły wstępne i końcowe można przeglądać na zarządzanej zaporze, lecz edycję parametrów można przeprowadzać tylko z poziomu systemu Panorama w zakresie zdefiniowanych ról administracyjnych. Lokalne reguły dotyczące urządzeń (znajdujące się pomiędzy regułami wstępnymi a regułami końcowymi) może edytować zarówno administrator lokalny, jak i administrator systemu Panorama po przełączeniu do kontekstu zapory lokalnej. Ponadto organizacja może używać współużytkowanych obiektów zdefiniowanych przez administratora systemu Panorama z odniesieniami do lokalnie zarządzanych reguł dotyczących urządzeń.
- **Administracja oparta na rolach:** Organizacje mogą korzystać z administracji opartej na rolach w celu przydzielania dostępu administracyjnego na poziomie funkcji (włączony, tylko do odczytu, wyłączony i widok ukryty) różnym pracownikom. Wybrani administratorzy mogą uzyskać odpowiedni dostęp do zadań zgodnych z ich stanowiskiem, a inni użytkownicy tylko dostęp do widoku ukrytego lub dostęp tylko do odczytu. Przykładem tego typu kontroli dostępu może być definiowanie różnych ról pracowników odpowiedzialnych za poszczególne zadania w przedsiębiorstwie, na przykład dla administratorów zabezpieczeń czy administratorów sieci. Wszelkie zmiany wprowadzane przez administratora są rejestrowane z informacjami, takimi jak godzina wystąpienia, imię i nazwisko administratora, użyty interfejs zarządzania (interfejs graficzny, interfejs wiersza poleceń, system Panorama), polecenie czy wykonane działanie.
- **Zarządzanie aktualizacjami oprogramowania, zawartości i licencji:** W miarę wzrostu rozmiarów wdrożonego systemu wiele organizacji dąży do zapewnienia uporządkowanej dystrybucji aktualizacji do poszczególnych elementów systemu. Na przykład zespoły ds. zabezpieczeń mogą wymagać centralnej kwalifikacji oprogramowania przed jego rozesłaniem za pośrednictwem systemu Panorama do wszystkich zapór. Dzięki systemowi Panorama można centralnie zarządzać procesem aktualizacji oprogramowania, zawartości (aktualizacji aplikacji, sygnatur antywirusowych, sygnatur zagrożeń, baz danych filtrów adresów URL itp.) oraz licencji.

Za pomocą szablonów, grup urządzeń, administracji opartej na rolach i zarządzania aktualizacjami organizacje mogą przydzielać odpowiednie uprawnienia dostępu do wszystkich funkcji zarządzania, tworzenia polityk, raportowania oraz rejestracji na poziomie globalnym i lokalnym, jak również narzędzi do wizualizacji.

System Panorama umożliwia organizacjom zrównoważenie centralnego i lokalnego zarządzania za pomocą szablonów, grup urządzeń, administracji opartej na rolach i zarządzania aktualizacjami.



Elastyczność wdrażania

Organizacje mogą wdrożyć system Panorama w postaci urządzenia fizycznego lub wirtualnego.

Urządzenie fizyczne

Organizacje preferujące wdrożenie systemu Panorama na specjalnym, wydajnym sprzęcie lub chcące rozdzielić w systemie Panorama funkcje zarządzania i rejestrowania dużych ilości danych mogą w tym celu zastosować urządzenie M-100. System Panorama działający na urządzeniu M-100 można wdrożyć następującymi metodami:

- **Wdrożenie centralne:** W tym scenariuszu wszystkie funkcje zarządzania i rejestrowania w systemie Panorama są realizowane przez jedno urządzenie (z opcją wysokiej dostępności).
- **Wdrożenie rozproszone:** Organizacja może wymagać rozdzielenia funkcji zarządzania i rejestrowania na wiele urządzeń. W takiej konfiguracji funkcje zostają rozdzielone na urządzenia menedżerów i agregatorów dzienników.
  - **Urządzenie menedżera systemu Panorama:** Urządzenie menedżera systemu Panorama odpowiada za obsługę zadań związanych z konfiguracją polityk i urządzeń we wszystkich zarządzanych urządzeniach. Urządzenie menedżera nie przechowuje danych dzienników lokalnie, ale do obsługi tych danych używa agregatorów dzienników. Urządzenie menedżera analizuje dane zapisane w agregatorach dzienników na potrzeby centralnej funkcji tworzenia raportów.
  - **Urządzenie agregatora dzienników systemu Panorama:** Organizacje charakteryzujące się dużymi ilościami danych dzienników oraz zaostrzonymi wymaganiami w zakresie przechowywania danych mogą wdrożyć specjalne urządzenia agregatora dzienników systemu Panorama, które gromadzą dane dzienników z wielu zarządzanych zapór.

Rozdzielenie funkcji zarządzania i agregowania dzienników umożliwia organizacjom zoptymalizowanie wdrożenia w celu spełnienia wymagań w zakresie skalowalności, a także wymagań organizacyjnych i geograficznych.

Urządzenie wirtualne

System Panorama można wdrożyć w postaci urządzenia wirtualnego na platformie VMware ESX(i), co zapewnia organizacjom możliwość kontynuowania inicjatyw w zakresie wirtualizacji oraz zmniejszania liczby urządzeń fizycznych ze względu na ograniczenia miejsca i kosztów w centrum danych. Urządzenie wirtualne można wdrożyć dwoma metodami:

- **Wdrożenie centralne:** Wszystkie funkcje zarządzania i rejestrowania w systemie Panorama są realizowane przez jedno urządzenie wirtualne (z opcją wysokiej dostępności).
- **Wdrożenie rozproszone:** Funkcja rozproszonej agregacji dzienników w systemie Panorama obsługuje szeroki wachlarz urządzeń fizycznych i wirtualnych.
  - **Urządzenie menedżera systemu Panorama:** Wirtualne urządzenie menedżera systemu Panorama odpowiada za obsługę zadań związanych z konfiguracją polityk i urządzeń we wszystkich zarządzanych urządzeniach.
  - **Urządzenie agregatora dzienników systemu Panorama:** Urządzenia agregatorów dzienników systemu Panorama odciążają moc obliczeniową poświęcaną na zbieranie i przetwarzanie danych dzienników. Można je wdrożyć w postaci fizycznego urządzenia M-100. Urządzenia wirtualnego nie można używać w roli agregatora dzienników systemu Panorama.

Opcje platformy sprzętowej i wirtualnej, a także możliwości połączenia lub rozdzielenia funkcji systemu Panorama zapewniają organizacjom maksymalną elastyczność w zakresie zarządzania wieloma zaporami firmy Palo Alto Networks w rozproszonym środowisku sieciowym.

PANORAMA — DANE TECHNICZNE

Liczba obsługiwanych urządzeń	Do 1000
Wysoka dostępność	Tryb aktywny/pasywny
Uwierzytelnianie administratora	Lokalna baza danych
	Serwer RADIUS

URZĄDZENIE DO ZARZĄDZANIA M-100 — DANE TECHNICZNE

PORTY WE-WY

- (1) port 10/100/1000, (3) porty 10/100/1000 (do wykorzystania w przyszłości), (1) port szeregowy konsoli DB9

PAMIĘĆ MASOWA (2 OPCJE)

- M-100 1 TB RAID: 2 dyski twarde z certyfikatem RAID w przypadku pamięci masowej RAID o pojemności 1 TB
- M-100 4 TB RAID: 8 dysków twardych o pojemności 1 TB z certyfikatem RAID w przypadku pamięci masowej RAID o pojemności 4 TB

ZASILANIE/MAKSYMALNY POBÓR MOCY

- 500 W/500 W

MAKS. BTU/H

- 1705 BTU/h

NAPIĘCIE WEJŚCIOWE (CZĘSTOTLIWOŚĆ WEJŚCIOWA)

- 100–240 V AC (50–60 Hz)

MAKS. POBÓR PRĄDU

- 10 A przy 100 V AC

MONTAŻ W SZAFIE (WYMIARY)

14,5 roku

ŚREDNI CZAS MIĘDZY AWARIAMI (MTBF)

- standardowa szafa 1U, 19 cali (wys. 4,3 cm x gł. 58,4 cm x szer. 43,7 cm)

MASA (SAMO URZĄDZENIE/W OPAKOWANIU TRANSPORTOWYM)

- 12,11 kg/15,88 kg

BEZPIECZEŃSTWO

- UL, CUL, CB

INTERFERENCJA ELEKTROMAGNETYCZNA (EMI)

- FCC — klasa A, CE — klasa A, VCCI — klasa A

ŚRODOWISKO

- Temperatura pracy: od 5 do 40°C (od 40 do 104°F)
- Temperatura w stanie spoczynku: od -40 do 65°C (od -40 do 149°F)

URZĄDZENIE WIRTUALNE — DANE TECHNICZNE

WYMAGANIA MINIMALNE SERWERA

- Dysk twardy o pojemności 40 GB
- 4 GB pamięci RAM
- Quad-Core CPU (2GHz+)

OBSŁUGIWANE PLATFORMY VMWARE

- VMware ESX 4.1 lub nowsza

OBSŁUGIWANE PRZEGLĄDARKI

- IE 7 lub nowsza
- Firefox 3.6 lub nowsza
- Safari 5.0 lub nowsza
- Chrome 11.0 lub nowsza

PRZECHOWYWANIE DZIENNIKÓW

- Dysk wirtualny VMware: maks. 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