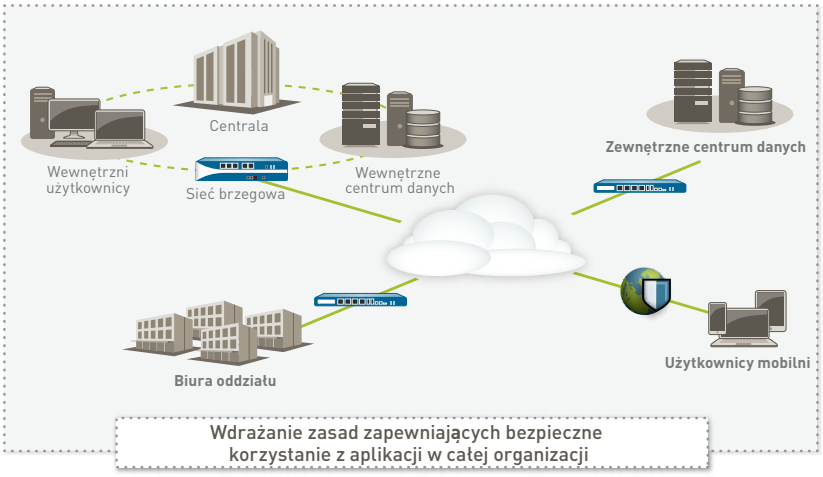
Informacje o zaporze nowej generacji firmy Palo Alto Networks

Fundamentalne zmiany, jakie zachodzą w dziedzinie aplikacji i zagrożeń komputerowych, a także w zachowaniach użytkowników i infrastrukturze sieciowej, prowadzą do stopniowego osłabienia ochrony zapewnianej dawniej przez tradycyjne, oparte na portach zapory. Wykonując codzienne zadania, użytkownicy korzystają z rożnych aplikacji i posługują się zróżnicowanymi urządzeniami. Tymczasem rozwój centrów danych oraz technologii wirtualizacji, mobilności i chmury wiąże się z koniecznością przemyślenia na nowo, jak zapewnić jednocześnie możliwość korzystanie z aplikacji i ochronę sieci.

Tradycyjne metody polegają na przykład na próbie zablokowania całego ruchu aplikacji poprzez zastosowanie stale poszerzanej listy technologii punktowych, będących dodatkami do zapory. Takie rozwiązanie może utrudniać prowadzenie działalności biznesowej. Z drugiej strony można próbować zezwolić na dostęp wszystkim aplikacjom, co również jest nie do przyjęcia ze względu na związane z tym zagrożenia dla firmy i bezpieczeństwa. Problem polega na tym, że tradycyjne, oparte na portach zapory, nawet te pozwalające na całkowitą blokadę aplikacji, nie oferują alternatywy dla żadnej z tych metod. Aby zachować równowagę między podejściem zakładającym całkowitą blokadę a podejściem umożliwiającym w pełni swobodny dostęp, trzeba stosować bezpieczne funkcje korzystania z aplikacji w oparciu o istotne dla firmy elementy, takie jak tożsamość aplikacji, dane osób korzystających z aplikacji czy rodzaj zawartości, jako kluczowe kryteria polityk bezpieczeństwa zapory.

Najważniejsze wymagania dotyczące bezpiecznego korzystania z aplikacji:

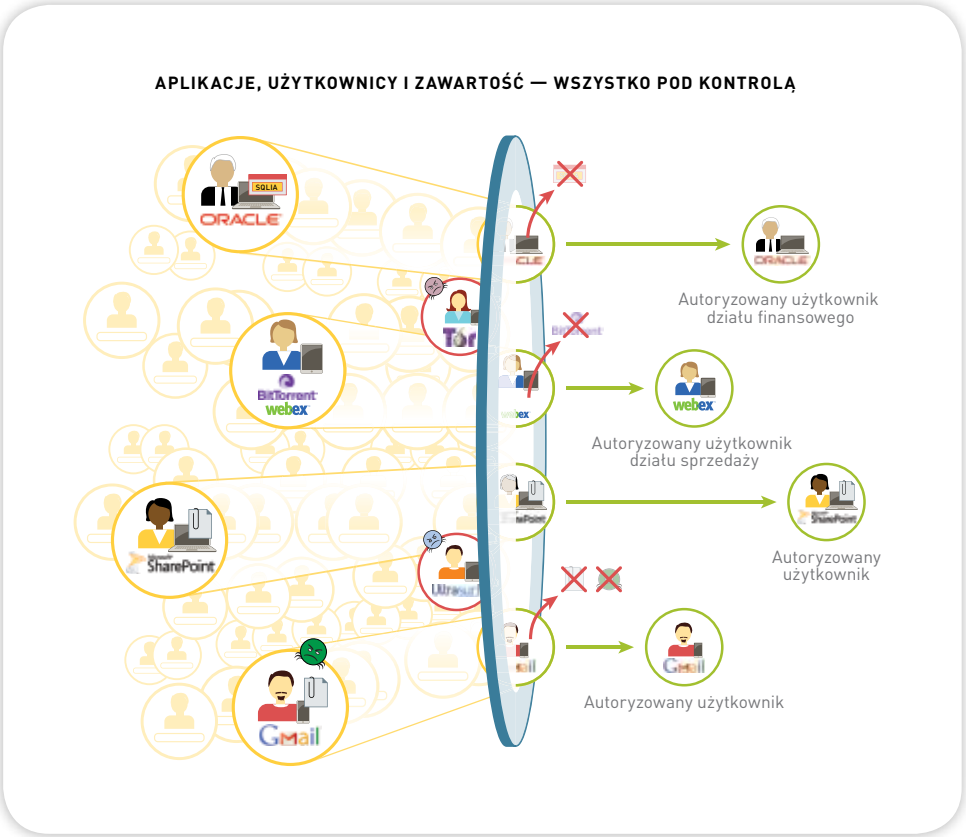
- **Identyfikacja aplikacji, a nie portów.** Klasyfikowanie ruchu sieciowego od razu po dotarciu do zapory w celu określenia tożsamości aplikacji bez względu na protokół, szyfrowanie czy taktykę unikową. Następnie wykorzystanie tej tożsamości jako podstawy wszystkich polityk bezpieczeństwa.
- **Powiązanie używania aplikacji z tożsamością użytkowników, a nie z adresem IP, bez względu na lokalizację lub urządzenie.** Wykorzystanie danych użytkowników i grup pochodzących z usług katalogowych i innych zasobów informacji o użytkownikach w celu wdrożenia spójnych polityk korzystania z aplikacji dla wszystkich użytkowników bez względu na lokalizację czy urządzenie.
- **Ochrona przed wszystkimi zagrożeniami — zarówno znanymi, jak i nieznanymi.** Zapobieganie znanym technikom wykorzystywania luk w zabezpieczeniach oraz działaniu oprogramowania złośliwego i szpiegującego oraz złośliwym adresom URL przy jednoczesnym analizowaniu ruchu pod kątem obecności wysoce ukierunkowanego i wcześniej nieznanego oprogramowania złośliwego, a także automatycznej ochrony przed jego działaniem.



paloalto NETWORKS
the network security company™

- **Uproszczenie zarządzania politykami bezpieczeństwa.** Bezpieczny dostęp do aplikacji i mniej działań administracyjnych dzięki łatwym w użyciu narzędziom graficznym, jednorodnym edytorze polityk, szablonom i grupom urządzeń.

Polityki zapewniające bezpieczne korzystanie z aplikacji pomagają zwiększyć bezpieczeństwo bez względu na miejsce wdrożenia. W sieci brzegowej można zmniejszyć liczbę zagrożeń dzięki zablokowaniu szeregu niechcianych aplikacji, a następnie aplikacje dopuszczone skanować w poszukiwaniu zagrożeń, zarówno tych znanych, jak i nieznanych. Jeśli chodzi o centrum danych — czy to tradycyjne czy zwirtualizowane — technologia korzystania z aplikacji oznacza, że aplikacje centrum danych mogą być używane tylko przez użytkowników autoryzowanych, co pozwala chronić zawartość centrum przed zagrożeniami i rozwiązywać problemy dotyczące bezpieczeństwa związane z dynamicznym charakterem infrastruktury wirtualnej. Odziały firmy i użytkownicy zdalni mogą być chronieni przy pomocy tego samego zestawu polityk korzystania z aplikacji wdrożonych w siedzibie głównej, co gwarantuje spójność polityk.



Korzystanie z aplikacji siłą napędową firmy

Bezpieczne korzystanie z aplikacji oferowane przez innowacyjne zapory firmy Palo Alto Networks pomaga zarządzać działalnością i stawiać czoła zagrożeniom bezpieczeństwa związanym z szybko rosnącą liczbą aplikacji w sieci firmowej. Udostępnianie aplikacji użytkownikom lub grupom użytkowników, zarówno lokalnym, mobilnym, jak i zdalnym, oraz ochrona ruchu sieciowego przed znanymi i nieznanymi zagrożeniami pozwala zwiększyć bezpieczeństwo, a jednocześnie rozwijać działalność.

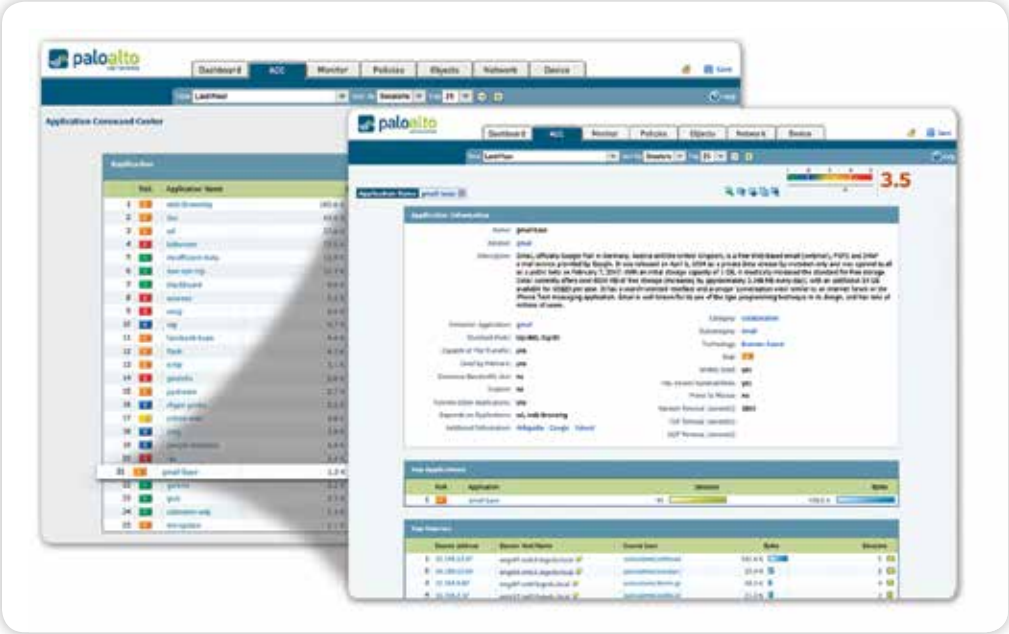
- **Możliwość stałej klasyfikacji wszystkich aplikacji na wszystkich portach.** Odpowiednia klasyfikacja ruchu sieciowego to podstawowy element każdej zapory, będący podstawą polityk zabezpieczeń. Obecnie aplikacje potrafią z łatwością omijać oparte na portach zapory, używając technik typu „port hopping", wykorzystując szyfrowanie SSL i SSH, przedostając się przez port 80 lub wykorzystując porty niestandardowe. Technologia App-ID rozwiązuje problem ograniczeń widoczności klasyfikacji ruchu, które są wadą zapór tradycyjnych, poprzez zastosowanie wielu mechanizmów klasyfikacji w strumieniu ruchu zaraz po dotarciu do zapory. Ma to na celu dokładne określenie tożsamości aplikacji wchodzącej do sieci, bez względu na rodzaj portu, szyfrowania (SSL lub SSH) czy stosowaną technikę unikową. Informacje na temat tego, które aplikacje przechodzą przez sieć, a nie tylko na temat portu i protokołu, stają się podstawą wszystkich decyzji dotyczących polityk zabezpieczeń. Niezidentyfikowane aplikacje, które zwykle stanowią niewielki procent ruchu, ale są potencjalnie groźne, poddawane są automatycznej kategoryzacji. Pozwala to na systematyczne rozwiązywanie problemów z bezpieczeństwem. Działania te mogą obejmować kontrolę polityk, badanie zagrożeń, tworzenie sygnatur App-ID dla niestandardowych aplikacji lub przechwytywanie pakietów w celu doskonalenia programowania sygnatur App-ID.

- **Uwzględnienie w politykach bezpieczeństwa użytkowników i urządzeń, a nie tylko adresów IP.** Tworzenie i zarządzanie politykami zabezpieczeń w oparciu o aplikację i tożsamość użytkownika, bez względu na urządzenie czy lokalizację, jest bardziej skuteczną metodą ochrony sieci niż techniki wykorzystujące wyłącznie port i adres IP. Integracja z szeroką gamą firmowych baz danych użytkowników pozwala na identyfikację tożsamości użytkowników systemów Microsoft Windows, Mac OS X, Linux, Android i iOS, którzy uzyskują dostęp do aplikacji. Użytkownicy mobilni i pracujący zdalnie są skutecznie chronieni przy pomocy tych samych spójnych polityk, które są stosowane w sieci lokalnej lub firmowej. Połączenie widoczności i kontroli aktywności użytkownika dotyczącej aplikacji oznacza, że można bezpiecznie udostępniać aplikacje Oracle, BitTorrent czy Gmail oraz wszelkie inne aplikacje w sieci bez względu na to, kiedy i w jaki sposób użytkownik uzyskuje do nich dostęp.

- **Ochrona przed wszystkimi zagrożeniami, zarówno znanymi, jak i nieznanymi.** Aby móc chronić współczesną sieć, trzeba zająć się różnego rodzaju znanymi metodami naruszeń, złośliwym oprogramowaniem i programami szpiegującymi, a także zupełnie nieznanymi i ukierunkowanymi zagrożeniami. Początkiem tego procesu jest zmniejszenie powierzchni narażonej na ataki sieci poprzez dopuszczenie określonych aplikacji i odrzucenie wszystkich pozostałych, czy to w sposób niejawny, przy użyciu strategii „odrzuć wszystko pozostałe", czy też w ramach polityk jawnych. Następnie do całego ruchu dopuszczonego można zastosować skoordynowaną ochronę przed zagrożeniami, polegającą na zablokowaniu znanych witryn złośliwego oprogramowania, programów wykorzystujących luki w zabezpieczeniach, wirusów, oprogramowania szpiegowskiego i złośliwych zapytań DNS w ramach operacji jednoprzebiegowej. Niestandardowe lub innego rodzaju nieznane złośliwe oprogramowanie jest aktywnie analizowane i identyfikowane poprzez wykonywanie nieznanych plików i bezpośrednie obserwowanie ponad 100 złośliwych zachowań w zwirtualizowanym środowisku sandbox. Po odkryciu nowego złośliwego oprogramowania następuje automatyczne wygenerowanie sygnatury zainfekowanego pliku i powiązanego z nim ruchu złośliwego oprogramowania oraz dostarczenie jej do użytkownika. Cała ta prewencyjna analiza wykorzystuje pełny kontekst aplikacji i protokołów, co gwarantuje wykrywanie nawet tych zagrożeń, które próbują ukrywać się przed mechanizmami zabezpieczeń w tunelach, danych skompresowanych czy portach niestandardowych.

Elastyczność wdrażania i zarządzania

Funkcjonalność bezpiecznego korzystania z aplikacji jest dostępna w ramach indywidualnie zaprojektowanej platformy sprzętowej lub w postaci zwirtualizowanej. W przypadku wdrażania kilku zapór Palo Alto Networks, czy to w formie sprzętowej, czy zwirtualizowanej, można zastosować narzędzie Panorama, które jest opcjonalnym rozwiązaniem do scentralizowanego zarządzania, zapewniającym widoczność wzorców ruchu oraz umożliwiającym wdrażanie polityk, generowanie raportów i dostarczanie aktualizacji zawartości z poziomu centralnej lokalizacji.



Widoczność aplikacji: Funkcja widoczności aktywności aplikacji oferuje przejrzysty, łatwy do odczytu format. Istnieje możliwość dodawania i usuwania filtrów w celu wyświetlenia dalszych informacji na temat aplikacji, jej funkcji i użytkowników.

Bezpieczne korzystanie z aplikacji: kompleksowe podejście

Bezpieczne korzystanie z aplikacji wymaga zastosowania kompleksowego podejścia do zabezpieczenia sieci i rozwoju firmy, którego podstawą jest gruntowna znajomość aplikacji w sieci: kim są użytkownicy, bez względu na platformę czy lokalizację, oraz jaką zwartość, jeżeli w ogóle, zawiera aplikacja. Dysponując bardziej kompletną wiedzą na temat aktywności sieci, można tworzyć bardziej skuteczne polityki zabezpieczeń, oparte na elementach aplikacji, użytkownikach i zawartości mających znaczenie dla firmy. Lokalizacja użytkowników, ich platforma i miejsce wdrażania zabezpieczeń — granica zabezpieczeń, tradycyjne lub zwirtualizowane centrum danych, oddział firmy lub użytkownik zdalny — mają minimalny lub zerowy wpływ na sposób tworzenia polityk. Teraz można bezpiecznie udostępnić dowolną aplikację i zawartość dowolnemu użytkownikowi.

Kompletna wiedza oznacza bardziej skuteczne polityki zabezpieczeń

Doświadczenie dotyczące optymalnych rozwiązań bezpieczeństwa wskazuje, że lepsza znajomość elementów sieci pozwala lepiej wdrażać szczelniejsze polityki zabezpieczeń. Na przykład, jeżeli administratorzy wiedzą, które dokładnie aplikacje przechodzą przez sieć – co nie jest możliwe w przypadku szerszego, opartego na portach ruchu sieciowego – mogą zezwolić na dostęp tylko tym aplikacjom, które przydają się w działalności firmy, i zablokować aplikacje niepożądane. Wiedza o tym, kim jest dany użytkownik, a nie tylko znajomość samego adresu IP, to kolejne kryterium, które pozwala bardziej precyzyjnie tworzyć polityki. Dzięki zaawansowanemu zestawowi graficznych narzędzi wizualizacyjnych administratorzy uzyskują pełniejszy obraz aktywności aplikacji i jej potencjalnego wpływu na bezpieczeństwo, dzięki czemu mogą podejmować lepsze decyzje, gdy chodzi o polityki zabezpieczeń. Aplikacje są stale klasyfikowane, a w miarę zmiany ich stanu odbywa się dynamiczne aktualizowanie graficznych podsumowań, dostępnych za pośrednictwem prostego w obsłudze graficznego interfejsu.

- Nowe lub nieznane aplikacje można szybko sprawdzić jednym kliknięciem, wyświetlając opis aplikacji, cechy jej aktywności i tożsamość korzystających z niej osób.
- Dodatkowe funkcje widoczności kategorii adresów URL, zagrożeń i wzorców danych umożliwiają uzyskanie kompletnego obrazu aktywności sieci.

- Nieznane aplikacje, które zwykle stanowią niewielki procent ruchu, ale są potencjalnie groźne, poddawane są kategoryzacji i analizie. Umożliwia to ustalenie, czy są one aplikacjami wewnętrznymi, niezidentyfikowanymi wcześniej aplikacjami komercyjnymi czy też aplikacjami stanowiącymi zagrożenie dla bezpieczeństwa.
- Najczęściej użytkownicy uzyskują dostęp do wybranych aplikacji, nierzadko potrzebnych im do realizacji codziennych zadań, co sprawia, że aplikacja, użytkownik i powiązana zawartość są ważniejsze dla firmy niż kiedykolwiek wcześniej. Dysponując bardziej kompletną wiedzą na temat elementów sieci, administratorzy mogą tworzyć polityki bezpiecznego korzystania z aplikacji.

Korzystanie z aplikacji i zmniejszanie ryzyka

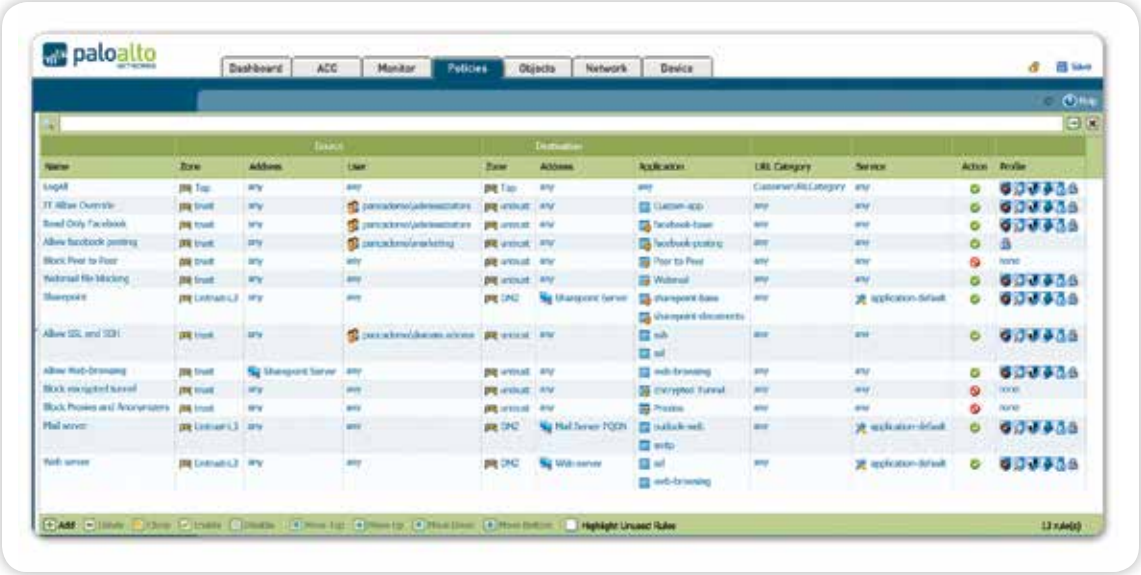
Funkcjonalność bezpiecznego korzystania z aplikacji wykorzystuje oparte na politykach kryteria decyzyjne, obejmujące aplikację/funkcję aplikacji, użytkowników i grupy oraz zawartość, aby umożliwić zachowanie równowagi między całkowitym blokowaniem wszystkich aplikacji a wysoce ryzykowanym podejściem zezwalającym na całkowicie swobodny dostęp.

Na granicy zabezpieczeń, na przykład w oddziałach firmy czy u użytkowników mobilnych i zdalnych, polityki korzystania z aplikacji skupiają się na identyfikowaniu całego ruchu, a następnie na selektywnym dopuszczaniu ruchu w oparciu o tożsamość użytkowników i skanowaniu ruchu sieciowego w poszukiwaniu zagrożeń. Przykładowe polityki zabezpieczeń:

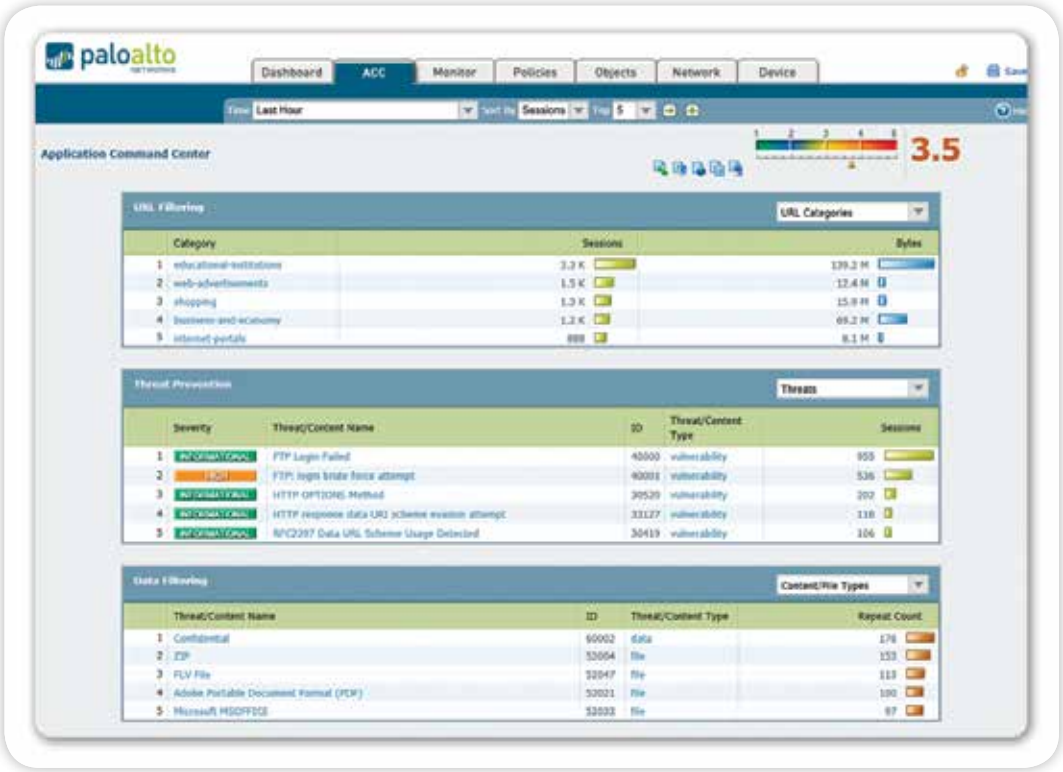
- Ograniczenie używania poczty elektronicznej i komunikatorów do kilku wariantów; rozszyfrowanie tych, które korzystają z SSL, kontrola ruchu pod kątem naruszeń i przesyłanie nieznanych plików do usługi WildFire w celu analizy i dodawania sygnatur.
- Dopuszczanie aplikacji i witryn strumieniowego przesyłania multimediów przy jednoczesnym zastosowaniu funkcji QoS i zabezpieczeń przed złośliwym oprogramowaniem w celu ograniczenia wpływu na aplikacje VoIP i ochrony sieci.
- Kontrola dostępu do serwisu Facebook poprzez zezwolenie na przeglądanie stron przez wszystkich użytkowników, zablokowanie wszystkich gier i dodatków społecznościowych serwisu oraz umożliwienie publikacji wpisów w serwisie Facebook tylko do celów marketingowych. Skanowanie całego ruchu w serwisie Facebook w poszukiwaniu złośliwego oprogramowania i prób wykorzystania luk w zabezpieczeniach.
- Kontrola korzystania z Internetu poprzez dopuszczanie i skanowanie ruchu dotyczącego witryn związanych z działalnością firmy przy jednoczesnym zablokowaniu dostępu do stron w sposób oczywisty niezwiązanych z działalnością; zarządzanie dostępem do wątpliwych witryn poprzez dostosowywalne blokowane strony.
- Ustanawianie spójnych zabezpieczeń poprzez przejrzyste wdrażanie takich samych polityk dla wszystkich użytkowników (lokalnych, mobilnych i zdalnych) przy użyciu funkcji GlobalProtect.
- Używanie niejawnej strategii „odrzuć wszystko pozostałe” lub jawne blokowanie niepożądanych aplikacji, takich jak P2P czy programów obchodzących zabezpieczenia oraz ruchu z określonych krajów w celu zmniejszenia ruchu aplikacji będącego źródłem zagrożeń dla firmy i bezpieczeństwa.

W centrach danych — zarówno tradycyjnych, zwirtualizowanych, jak i mieszanych — funkcje korzystania z aplikacji polegają przede wszystkim na zatwierdzaniu aplikacji, szukaniu szkodliwych aplikacji i ochronie danych.

- Odizolowanie opartego na systemie Oracle repozytorium numerów kart kredytowych we własnej strefie bezpieczeństwa; kontrola dostępu do grup finansowanych; kierowanie ruchu do portów standardowych; kontrola ruchu pod kątem luk w zabezpieczeniach aplikacji.
- Zezwolenie na dostęp do centrum danych tylko zespołowi IT za pomocą stałego zestawu aplikacji do zarządzania zdalnego (np. SSH, RDP, Telnet) w portach standardowych.
- Zezwolenie na korzystanie z funkcji administracji programu SharePoint firmy Microsoft tylko firmowemu zespołowi administracyjnemu oraz zezwolenie na korzystanie z dokumentów programu SharePoint wszystkim pozostałym użytkownikom.



Ujednolicony edytor polityk: Znany z poprzednich wersji wygląd i obsługa pozwala na szybkie tworzenie i wdrażanie polityk kontrolujących aplikacje, użytkowników i zawartość.



Widoczność zawartości i zagrożeń: Wyświetlanie adresów URL, zagrożeń i przesyłu plików/danych w przejrzystym, łatwym do odczytu formacie. Możliwość dodawania i usuwania filtrów w celu wyświetlania dalszych informacji o poszczególnych elementach.

Ochrona udostępnionych aplikacji

Bezpieczne korzystanie z aplikacji polega na zezwalaniu na dostęp do określonych aplikacji, następnie stosowaniu konkretnych polityk w celu zablokowania znanych nadużyć, złośliwego oprogramowania i programów szpiegowskich (znanych i nieznanych) oraz kontrolowaniu przesyłania plików lub danych i aktywności związanej z przeglądaniem Internetu. Popularne taktyki omijania zabezpieczeń, takie jak „port hopping" czy tunelowanie, zwalczane są za pomocą polityk prewencyjnych wykorzystujących kontekst aplikacji i protokołów wygenerowany przez dekodery w funkcji App-ID. Z kolei rozwiązania UTM wykorzystują oparte na silosach metody zapobiegania zagrożeniom, które stosowane są do każdej

funkcji, zapory, IPS, antywirusa, filtrowania URL, całego ruchu sieciowego bez uwzględnienia kontekstu, co czyni je bardziej podatnymi na techniki unikowe.

- **Blokowanie znanych zagrożeń: IPS i sieciowe oprogramowanie antywirusowe/antyspyware.** Jednorodny format sygnatur i oparty na technologii strumieniowania mechanizm skanowania pozwala chronić sieć przed wieloma rodzajami zagrożeń. System zapobiegania intruzom (IPS) obsługuje przypadki wykorzystania luk zabezpieczeń polegające na blokowaniu sieci i zachodzące w warstwie aplikacji, a także chroni przed przepełnieniem buforu, atakami DoS i skanowaniem portów. Ochrona antywirusowa/antyspyware blokuje miliony odmian złośliwego oprogramowania, jak również generowany przez nie ruch command-and-control, wirusy PDF i złośliwe oprogramowanie ukryte w plikach skompresowanych lub w ruchu sieci Web (skompresowane dane HTTP/HTTPS). Oparte na politykach rozszyfrowanie SSL we wszystkich aplikacjach i portach chroni przed złośliwym oprogramowaniem przechodzącym przez aplikacje szyfrowane metodą SSL.
- **Blokowania nieznanego, ukierunkowanego złośliwego oprogramowania: Wildfire™.** Nieznane i ukierunkowane złośliwe oprogramowanie jest identyfikowane i analizowane przez funkcję WildFire, która bezpośrednio wykonuje i obserwuje nieznane pliki w zwirtualizowanym środowisku sandbox w chmurze. WildFire monitoruje ponad 100 złośliwych zachowań, a wyniki analiz trafiają natychmiast do administratora w formie alertu. Opcjonalna subskrypcja funkcji WildFire oferuje zwiększoną ochronę, funkcję zapisywania w dziennikach i raportowanie. Posiadacze subskrypcji otrzymują ochronę w ciągu godziny od odkrycia nowego złośliwego oprogramowania w dowolnym miejscu na świecie, co skutecznie zapobiega rozprzestrzenianiu się tego rodzaju oprogramowania, zanim dotrze ono do użytkownika. Subskrypcja wiąże się także z dostępem do zintegrowanej funkcji zapisywania w dziennikach i raportowania produktu WildFire oraz interfejsu API umożliwiającego przesyłanie próbek do chmury WildFire w celu analizy.
- **Identyfikacja hostów zainfekowanych botami.** Funkcja App-ID pozwala klasyfikować wszystkie aplikacje, we wszystkich portach, w tym cały nieznany ruch, który często może stanowić źródło zagrożeń lub anomalii w sieci. Raport dotyczący zachowania się botów zestawia nieznany ruch, podejrzane zapytania DNS i URL oraz szereg różnych nietypowych zachowań w sieci, dając obraz urządzeń, które mogą być zainfekowane złośliwym oprogramowaniem. Wyniki są wyświetlane w formie listy potencjalnie zainfekowanych hostów, które można zanalizować jako podejrzane elementy sieci botnet.
- **Ograniczanie nieautoryzowanego przesyłania plików i danych.** Funkcje filtrowania danych pozwalają administratorom na wdrażanie polityk zmniejszających ryzyko związane z nieautoryzowanym przesyłaniem plików i danych. Przesyłanie plików można kontrolować, sprawdzając zwartość pliku (a nie tylko jego rozszerzenie) w celu określenia, czy można zezwolić na operację przesyłania czy też nie. Pliki wykonywalne, często występujące w atakach polegających na niepożądanym pobieraniu, można blokować, chroniąc sieć przed niewidocznym rozprzestrzenieniem się złośliwego oprogramowania. Funkcje filtrowania danych wykrywają i kontrolują przepływ poufnych danych (numery kart kredytowych, numery ubezpieczenia czy też innego rodzaju indywidualnie określone numery prywatne).
- **Kontrola korzystania z Internetu.** W pełni zintegrowany, dostosowywalny mechanizm filtrowania adresów URL umożliwia administratorom stosowanie granularnych polityk przeglądania sieci Web, które są uzupełnieniem funkcji widoczności aplikacji i polityk kontroli oraz chronią firmę przed wszelkiego rodzaju problemami dotyczącymi zgodności z przepisami prawnymi i normami produktywności. Ponadto, do budowania polityk bezpieczeństwa można włączyć kategorie URL, aby uzyskać dodatkową granularność kontroli rozszyfrowywania SSL, funkcji QoS lub innych elementów będących podstawami innych reguł.

Ciągłe zarządzanie i analiza

Doświadczenie dotyczące optymalnych rozwiązań bezpieczeństwa wskazuje, że administratorzy powinny zachować równowagę między proaktywnym zarządzaniem zaporą, czy to w zakresie pojedynczego urządzenia czy setek urządzeń, a reagowaniem poprzez badanie, analizowanie i zgłaszanie incydentów dotyczących bezpieczeństwa.

- **Zarządzanie:** Każdą platformą Palo Alto Networks można zarządzać osobno za pośrednictwem interfejsu wiersza poleceń lub wyposażonego we wszystkie funkcje interfejsu graficznego. W przypadku dużych wdrożeń produkt Panorama może być udostępniony na zasadzie licencyjnej i wdrażany jako scentralizowane rozwiązanie do zarządzania, pozwalające pogodzić globalne, scentralizowane sterowanie z elastycznością w zakresie polityk lokalnych, za pomocą takich funkcji jak szablony i polityki współdzielone. Dodatkowa obsługa opartych na standardach narzędzi, takich jak SNMP i wykorzystujący architekturę REST interfejs API pozwala na integrację z narzędziami do zarządzania innych firm. Zarówno interfejs graficzny urządzenia, jak i interfejs produktu Panorama mają taki sam wygląd i oferują ten sam komfort użytkowania, dzięki czemu nie ma potrzeby dodatkowego szkolenia użytkowników w przypadku migracji. Administratorzy mogą korzystać z dowolnego z interfejsów i w każdym momencie wprowadzać dowolne zmiany bez obaw o problemy związane z synchronizacją. We wszystkich narzędziach zarządzania obsługiwana jest administracja oparta na rolach, umożliwiająca przypisywanie funkcji konkretnym osobom.
- **Raportowanie:** Można używać wstępnie zdefiniowanych raportów w postaci niezmienionej lub dostosowanej oraz pogrupowanych w formie jednego raportu, zgodnie z wymaganiami. Wszystkie raporty można eksportować do formatu CSV lub PDF, otwierać i wysyłać pocztą elektroniczną według ustalonego harmonogramu.
- **Zapisywanie w dziennikach:** Funkcja filtrowania dzienników w czasie rzeczywistym umożliwia kontrolowanie każdej sesji w sieci. Wyniki filtrowania dzienników można eksportować do pliku CSV lub wysyłać do serwera syslog do archiwizacji offline lub dodatkowej analizy.

Indywidualnie zaprojektowana platforma sprzętowa lub platforma zwirtualizowana

Firma Palo Alto Networks oferuje pełną gamę indywidualnie zaprojektowanych platform sprzętowych, począwszy od modelu PA-200 – przeznaczonego dla zdalnych biur korporacyjnych, do modelu PA-5060 – zaprojektowanego dla wysokiej klasy centrów danych. Architektura platform została oparta na jednoprzebiegowym oprogramowaniu i wykorzystuje przetwarzanie specyficzne dla funkcji w zakresie połączeń sieciowych, zabezpieczeń, zapobiegania zagrożeniom i zarządzania, odznaczając się przy tym stabilnym i wydajnym działaniem. Ta sama funkcjonalność zapory, w jaką wyposażone są platformy sprzętowe, jest dostępna w zaporze wirtualnej serii VM, która zabezpiecza zwirtualizowane i oparte na chmurze środowiska obliczeniowe z zastosowaniem tych samych polityk do komputerów sieci brzegowej, jak i zapór w biurach zdalnych.

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