Citrix Application Firewall™
Product Overview

Wszechstronna ochrona danych oraz serwerów aplikacji i usług sieciowych

Citrix Application Firewall™ to wysokowydajne, zaawansowane urządzenie zabezpieczające, które blokuje znane i nieznane ataki wobec aplikacji i usług sieciowych. Citrix Application Firewall wprowadza w życie pozytywny model bezpieczeństwa, który zamiast polegać na sygnaturach ataków, akceptuje jedynie właściwe zachowanie aplikacji. Application Firewall analizuje cały ruch dwukierunkowy, w tym informacje zaszyfrowane protokołem SSL, zapewniając ochronę przed 16 klasami zagrożeń dla aplikacji sieciowych bez żadnych modyfikacji w aplikacjach.

Zapora Citrix Application Firewall jest dostępna jako rodzina specjalnie zaprojektowanych urządzeń, spełniających dowolną potrzebę wdrożeniową, i występuje w dwóch edycjach, umożliwiających aktualizacje w miarę jak zagrożenia, aplikacje i zabezpieczenia stają się coraz bardziej skomplikowane. Produkt ten można instalować pojedynczo lub w połączeniu z systemami optymalizacji dostarczania aplikacji internetowych Citrix® NetScaler®, dzięki czemu można połączyć korzyści z optymalizacji aplikacji i ich wszechstronnej ochrony.

Odpowiedź na obecne wyzwania związane z bezpieczeństwem

Infrastruktury bezpieczeństwa oparte wyłącznie na urządzeniach zabezpieczających na poziomie sieci, takich jak zapory sieciowe czy systemy zapobiegania włamaniom, nie mogą w pełni zabezpieczać przed atakami w warstwie aplikacji, przez co aplikacje i serwery pozostają narażone na wiele znanych i nieznanych zagrożeń. Application Firewall kompleksowo stawia czoła tym wyzwaniom, zapewniając scentralizowane zabezpieczenie warstwy aplikacji dla wszystkich aplikacji i usług sieciowych.

Zaleta pozytywnego modelu bezpieczeństwa

Citrix Application Firewall wprowadza w życie pozytywny model bezpieczeństwa, zapewniając właściwe funkcjonowanie aplikacji. Zamiast polegać na sygnaturach ataków lub technikach rozpoznawania wzorców, pozytywny model zabezpieczenia akceptuje jedynie właściwe zachowanie aplikacji, blokując jako złośliwe wszelkie nietypowe procedury. Jest to jedyny sprawdzony sposób natychmiastowej ochrony przed nowymi rodzajami jeszcze nieznanych zagrożeń.

Silna ochrona obiektów biznesowych

Citrix Application Firewall w czasie rzeczywistym zapobiega przypadkowym ujawnieniom poufnej zawartości aplikacji, czego skutkiem mogłaby być kradzież tożsamości i oszustwo. Moduły ochrony

CITRIX®

obiektów biznesowych pomagają chronić bezpieczeństwo zarówno wcześniej zdefiniowanych obiektów takich jak numery kart kredytowych, jak również obiektów zdefiniowanych przez administratora. Dzięki wykrywaniu przypadkowych ujawnień i blokowaniu lub przepisywaniu treści, moduły ochrony obiektów biznesowych pomagają zachować zgodność z ustawowymi regulacjami dotyczącymi ochrony prywatności.

Dopasowanie polityk bezpieczeństwa dzięki modułowi Citrix Adaptive Learning

Citrix Application Firewall zawiera moduł Adaptive Learning trzeciej generacji, który analizuje podstawowe aspekty zachowania się aplikacji. Gdy wykryte (ustalone) zostanie właściwe zachowanie aplikacji, Application Firewall generuje zrozumiałe rekomendacje dotyczące polityk bezpieczeństwa, co pozwala menedżerom ds. bezpieczeństwa dobrze zrozumieć poprawne zachowanie się aplikacji. Dostosowane reguły bezpieczeństwa i rygorystyczna kontrola dostępu mogą być wówczas stosowane w stosunku do każdej aplikacji.

Tłumaczenie i przepisywanie adresów URL

Citrix Application Firewall chroni przed rekonesansem informacyjnym w witrynie internetowej z dwukierunkowym tłumaczeniem adresu URL, umożliwiając organizacjom całkowite ukrycie nazw swych domen przy publikowaniu swych serwisów.

Najlepsza wydajność w branży

Wydajność Citrix Application Firewall przekracza wydajność najszybszych serwerów internetowych i zapora ta może istotnie zwiększyć wydajność aplikacji oraz czas reakcji poprzez przejęcie z serwerów internetowych obciążenia pamięci i mocy obliczeniowej związanych z zarządzaniem połączeniami TCP. Komunikacja pomiędzy zaporą Application Firewall a serwerem odbywa się z wykorzystaniem niewielkiego zestawu trwałych połączeń TCP.

Specjalne, oparte na krzemie rozwiązanie sprzętowe do szyfrowania SSL pozwala wykryć szkodliwy ruch w zaszyfrowanych tunelach. Przeniesienie szyfrowania SSL i generowania kluczy może zwiększyć ogólną wydajność aplikacji poprzez odciążenie serwerów z wykonywania tych operacji. Opcjonalnie dostępne jest również pełne szyfrowanie komunikacji skierowanej z zapory Application Firewall do serwerów aplikacyjnych.

Klaster Application Firewall zapewnia duży poziom dostępności i liniowy wzrost wydajności wraz z rozbudową klastra.

Scentralizowane zabezpieczenie wszystkich aplikacji i usług sieciowych

Zapora Application Firewall może ochraniać całą infrastrukturę aplikacji i usług sieciowych organizacji, dzięki całkowitemu administracyjnemu oddzieleniu reguł bezpieczeństwa aplikacji, ich kontroli, szczegółów raportowania i danych z dziennika aplikacji.

Elastyczne dostosowanie się do zmiennych potrzeb biznesowych

Citrix Application Firewall Standard Edition zapewnia pełną ochronę przed najczęstszymi i najbardziej niebezpiecznymi zagrożeniami dla aplikacji internetowych, wydajne zabezpieczenie aplikacji internetowych i usług wykorzystujących technologię XML, oraz pełną ochronę przed kradzieżą danych. Produkt ten można bez przeszkód rozszerzyć do edycji Enterprise Edition.

Citrix Application Firewall Enterprise Edition zawiera dodatkowo zaawansowane funkcje uczenia się, które zapewniają ochronę przed najbardziej złożonymi atakami w warstwie aplikacji, zabezpieczając przed atakami wymierzonymi w konkretne sesje użytkownika (co jest konieczne w przypadku aplikacji stosowanych w e-handlu, bezpiecznych sieci extranet i bankowości elektronicznej) oraz zapewniają bardziej precyzyjną kontrolę nad politykami bezpieczeństwa aplikacji.

Zapora Citrix Application Firewall dostępna jest na wielu platformach sprzętowych, dzięki czemu spełnia wymogi wydajności i dostępności praktycznie każdej organizacji – od małej firmy po wielkie centra danych. W sprzedaży dostępne są również modele zgodne z normą FIPS (Federal Information Processing Standard) 140-2 na poziomie 3.

Kluczowe korzyści

Ochrona poufnych danych osobowych klientów.
Chroni dane znajdujące się za infrastrukturą sieciową przed kradzieżą tożsamości oraz wykorzystaniem rachunków bankowych i kart kredytowych.

Eliminuje możliwość utraty danych, o których zgodnie z przepisami rządowymi należy powiadamiać klienta.

Ochrona źródeł dochodów z działalności online.
Gwarantuje sprawne funkcjonowanie witryn i usług internetowych poprzez zapobieganie atakom typu odmowa świadczenia usługi (DoS, Denial of Service) w warstwie 7.

Funkcja Application Learning zapewnia ochronę poprzez blokowanie nieznanych jeszcze zagrożeń, które dla tradycyjnych zabezpieczeń mogą wydawać się bezpiecznymi obiektami.

Utrzymuje relację zaufania pomiędzy konsumentem a dostawcą, dzięki zapobieganiu atakom typu cross-site scripting (XSS).

Ochrona przed erozją marki.
Zapewnia integralność treści, dzięki zabezpieczeniu przed podmianą strony internetowej.

Cechy kluczowe

Ochrona przed 16 klasami zagrożeń sieciowych

- Przepełnienie bufora (buffer overflow)
- Manipulacje parametrami CGI-BIN
- Manipulacje z wykorzystaniem ukrytego pola formularza
- Pomijanie uwierzytelniania (forceful browsing)
- Infekowanie plików cookie lub sesji
- Uszkodzone listy kontroli dostępu lub słabe hasła
- Cross-site scripting (XSS)
- Wstrzyknięcie poleceń (Command injection)
- Wstrzyknięcie SQL (SQL injection)
- Błąd wywołujący wypłynięcie informacji niejawnych
- Nieprawidłowe stosowanie kryptografii
- Nieprawidłowa konfiguracja serwera
- Tylne wejścia i opcje debugowania
- Podmiana strony WWW
- Znane luki systemowe
- Ataki typu „zero-day”

Wszechstronna ochrona aplikacji i usług sieciowych

Dogłębna inspekcja strumienia

- Analiza ruchu w obu kierunkach
- Kontrola nagłówków i pól tekstowych HTTP i HTML
- Pełne parsowanie HTML
- Ekstrakcja semantyczna
- Zachowanie informacji o sesji i kontrola stanu
- Niezależność od protokołów

Ochrona pól formularzy HTML

- Zwracanie żądanych pól
- Blokada dodawania pól
- Blokowanie pól tylko do odczytu i ukrytych
- Zgodność listy rozwijanej i pola przełączników
- Blokowanie maksymalnej długości pól formularzy

Zabezpieczenia przed zatruwaniem plików cookie

- Zabezpiecza plików cookie przed modyfikacją

Ochrona przed pomijaniem uwierzytelniania

- Wymuszenie prawdziwego adresu URL

Integralność treści aplikacji sieciowych

- Zabezpieczenie przed podmianą strony WWW
- Blokowanie określonych słów
- Akceptowanie określonych słów

Pełne przeniesienie szyfrowania SSL poza serwer

- Deszyfruje ruch przed inspekcją
- Szyfruje ruch przed inspekcją
- Konfigurowalne szyfrowanie zaplecza
- Dostępne platformy spełniające normę FIPS 140-2 na poziomie 3
- Obsługa certyfikatów klienckich

Uproszczone zarządzanie i wdrożenie

Interfejs użytkownika

- Bezpieczny sieciowy interfejs użytkownika
- Dostęp do interfejsu wiersza polecenia przez SSH

Zarządzanie siecią

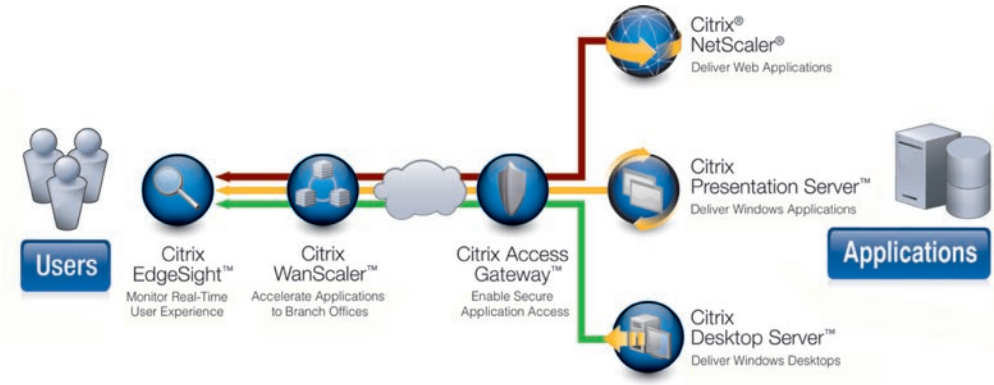
- Protokół SNMP
- Logowanie przez syslog

Specyfikacja techniczna

Model urządzenia	7000	12000
Rozmiary	1,8” (4,4 cm) W x 17,3” (43,8 cm) S x 18,8” (47,6 cm) G	3,5” (8,8 cm) W x 17” (42,4 cm) W x 24” (61 cm) G (2U)
Waga	28 funtów (12,7 kg)	52 funty (23,6 kg)
Zasilanie	Prąd przemienny w pełnym zakresie: 90–264 V, 47–6 Hz, 335 W	Prąd przemienny w pełnym zakresie: 90–264 V, 47–6 Hz, 335 W
Porty sieciowe	6 x 10/100 BASE-T 2 x 10/100/1000 BASE-T	8 x 1 Gbit miedziany port SFP 1 x 10/100 BASE-T
Warunki eksploatacji	Temperatura i wilgotność 0–50°C, 5–95%	Temperatura i wilgotność 0–50°C, 5–95%
Certyfikaty i znaki zgodności z normami	Emisje: FCC (część 15 klasa A), DoC, CE, VCCI, CNS, AN/NES Bezpieczeństwo: TUV-C, US	Emisje: FCC (część 15 klasa A), DoC, CE, VCCI, CNS, AN/NES Bezpieczeństwo: TUV-C, US
Gwarancja sprzętowa	1 rok	1 rok

Sześć kluczowych elementów wydajnego systemu zdalnego dostępu do aplikacji

Dostęp do aplikacji dla wszystkich użytkowników – najwyższa wydajność, bezpieczeństwo i elastyczność, najniższy koszt.



Citrix® NetScaler® do dostarczania aplikacji internetowych — zoptymalizuj wszystkie aplikacje internetowe, korzystając ze zintegrowanego rozwiązania sieciowego, które zwiększa wydajność, poprawia bezpieczeństwo i zdecydowanie zmniejsza obciążenie serwerów.

Citrix Presentation Server™ do dostarczania aplikacji działających w systemie Windows — możesz zaoszczędzić miliony na kosztach administracji i wyeliminować zagrożenia dla danych, instalując aplikacje Windows w centrum obliczeniowym, a następnie udostępniając je użytkownikom przez sieć w postaci zwirtualizowanej lub strumieniowej.

Citrix Desktop Server™ do dostarczania pulpitów — zmniejsz koszty, nakłady pracy administracyjnej i zagrożenie bezpieczeństwa związane z pracą na stacjach roboczych, wirtualnie dostarczając pulpity Windows z centrum danych; w ten sposób poprawisz także komfort użytkowników.

Citrix Access Gateway™ do bezpiecznego dostępu do aplikacji — udostępnij pojedynczy, bezpieczny punkt dostępu do#wszystkich aplikacji, który automatycznie dostosowuje zasady dostępu w zależności od scenariuszy użytkownikat.

Citrix WanScaler™ do przyspieszania aplikacji używanych przez użytkowników w oddziałach — natychmiast popraw wydajność aplikacji dostarczanych przez sieci WAN, zmniejszając jednocześnie zużycie pasma nawet o 75%.

Citrix EdgeSight™ do monitorowania działania systemu z perspektywy użytkowników — zagwarantuj, że wszystkie aplikacje zawsze działają zgodnie z określonymi parametrami biznesowymi, monitorując ich wydajność z perspektywy użytkowników.

Citrix Worldwide

Worldwide headquarters

Citrix Systems, Inc.
851 West Cypress Creek RoadFort
Lauderdale, FL 33309
USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000

European headquarters

Citrix Systems International GmbH
Rheinweg 9, 8200 Schaffhausen
Switzerland
Tel: +41 (0)52 6 35 77-00

Asia / Pacific headquarters

Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street, Central
Hong Kong
Tel: +852 2100 5000

Citrix Online Division

Citrix Online Division
5385 Hollister Avenue
CA 93111, Santa Barbara
USA
Tel: +1 (805) 690 6400

Selected European subsidiaries

Citrix Systems GmbH
Am Söldnermoos 17
85399 Hallbergmoos / München
Germany
Tel: +49 (0)811 83-0000

Citrix Systems Poland Sp. z o.o.
Warsaw Financial Centre
ul. E. Plater 53
00-113 Warsaw
Poland
Tel: +48 (22) 528 6615

Representative office
of Citrix Systems Int. GmbH
Regus BC, Smolensky Passage
Smolenskaya sq.,3
121099 Moscow
Russia
Tel: +7 (495) 937 8249

www.citrix.com

Informacje o firmie Citrix:
Citrix Systems (NASDAQ: CTXS) jest globalny liderem i najbardziej zaufanym dostawcą infrastruktury do dostarczania aplikacji. Ponad 200 tys. organizacji z całego świata polega na firmie Citrix w zakresie dostarczania dowolnych aplikacji do użytkowników w dowolnym miejscu, przy zachowaniu najwyższej wydajności, bezpieczeństwa i najniższych kosztów. Do klientów firmy Citrix należy 100% firm z listy Fortune100 i 98% z listy FortuneGlobal500, a także setki tysięcy małych przedsiębiorstw i zaawansowanych użytkowników. Citrix ma około 6200 partnerów w ramach kanału dystrybucyjnego i sojuszu, działających w ponad 100 krajach. Roczne przychody wyniosły w 2006 r. 1,1 miliarda USD. Więcej informacji można uzyskać na stronie www.citrix.com.

©2007 Citrix Systems, Inc. Wszelkie prawa zastrzeżone. Citrix®, Citrix Application Firewall™, Citrix Presentation Server™, Citrix Application Gateway™, Citrix Access Gateway™, Citrix Password Manager™, NetScaler®, AppCache™, AppCompress™, AppExpert™, Request Switching®, GoToMeeting™, GoToAssist™, GoToMyPC® oraz Deep Stream Inspection™ są znakami towarowymi firmy Citrix Systems, Inc. i/lub jednej lub więcej firm od niej zależnych i mogą być zarejestrowane w Biurze Patentów i Znaków Towarowych USA (United States Patent and Trademark Office) i w innych krajach. Windows® jest zarejestrowanym znakiem towarowym firmy Microsoft Corporation w Stanach Zjednoczonych. UNIX® jest zarejestrowanym znakiem towarowym konsorcjum The Open Group w Stanach Zjednoczonych i innych krajach. Wszystkie inne znaki towarowe i zarejestrowane znaki towarowe należą do swoich właścicieli.