

## Spis treści:

- 2 Generator polityk oparty na prawdziwym ruchu
- 2 Ochrona „Out-of-the-Box”
- 2 Wymuszanie
- 2 Zintegrowany XML Firewall
- 2 Ochrona danych i maskowanie
- 2 Integracja z WhiteHat Sentinel
- 3 Uaktualnienia sygnatur
- 3 Zabezpieczenie protokołów SMTP i FTP
- 3 Wszeczhronna ochrona aplikacji
- 4 Specyfikacja platform sprzętowych



## Chroń swoją firmę za pomocą narzędzia nowej generacji do zabezpieczania aplikacji

Wraz z rosnącym ruchem aplikacyjnym w sieci światowej, coraz większa ilość wrażliwych danych jest wystawiona na nowe zagrożenia adresujące zarówno stacje klientów, serwery jak i same dane. Zagrożenia i związane z nimi ataki coraz częściej dotyczą warstwy aplikacyjnej i mogą zawierać wyrafinowane próby włamań wewnątrz samej metody dostępu i protokołu jak np. HTTP, XML, XSS, buffer overflow, SQL injection.

F5 BIG-IP Application Security Manager (ASM) jest zaawansowanym rozwiązaniem rodziny firewalli aplikacyjnych (Web Application Firewall) dostarczającym kompleksowej ochrony aplikacji webowych, znacząco redukujący i łagodzący ryzyko utraty lub uszkodzenia danych, własności intelektualnej czy też samej aplikacji. BIG-IP ASM chroni kapitał i reputację organizacji, dostarcza ochronę oraz adresuje kluczowe regulacje prawne takie jak PCI DSS, HIPAA, SOX. BIG-IP ASM zapewnia najbardziej wszechstronną ochronę informacji personalnych (numery kart kredytowych, numery kont, PESEL itd.) poprzez kontrolowanie dostępu do informacji na poziomie każdego zapytania/odpowiedzi HTTP. Wraz z BIG-IP ASM otrzymujemy kompletne rozwiązanie redukujące potrzebę używania wielu innych urządzeń, zmniejszające koszty zarządzania i zwiększające poufność, dostępność i integralność krytycznych procesów i aplikacji.

### Kluczowe korzyści:

**Zgodność z przemysłowymi standardami bezpieczeństwa** – wbudowana ochrona umożliwia przedsiębiorstwom na osiągnięcie zgodności ze standardami bezpieczeństwa takimi jak PCI DSS, HIPAA, SOX w efektywny sposób

**Redukcja ryzyka i szybka naprawa** – zaawansowany automatyczny generator polityk jest w stanie szybko naprawić nowoodkryte podatności, redukując czas, ryzyko i koszt związany z naprawą samej aplikacji przez programistów

**Ochrona „Out-of-the-Box”** – wbudowane, szybkie polityki zapewniają natychmiastową ochronę przy minimalnej konfiguracji dla każdej aplikacji webowej

**Centralne logowanie zdarzeń bezpieczeństwa** – logowanie wszystkich zdarzeń HTTP –

wewnętrznie lub zewnętrznie – do centralnego serwera zdarzeń gdzie logi są zbierane i mogą być analizowane

**Podniesienie sprawności biznesowej** – skoncentrowany na szybkim wdrożeniu nowych aplikacji i procesów za pomocą automatycznych, dokładnych polityk

**Ochrona danych i poprawa wydajności działania aplikacji** – polepsza prędkość działania aplikacji i umożliwia jej lepszą skalowalność – dzięki systemowi operacyjnemu F5 TMOS, możliwości terminacji SSL na urządzeniu, cachowaniu, kompresji, optymalizacji TCP i innych

**Ochrona na poziomie sieci, protokołu i aplikacji** – zawarty filtr pakietów, inspekcja i możliwość manipulacji pakietami, architektura proxy

## Generator polityk oparty na prawdziwym ruchu

Sercem BIG-IP ASM jest dynamiczny generator polityk, który jest odpowiedzialny za automatyczną naukę i stworzenie polityki. Podczas przepływu ruchu przez BIG-IP ASM, generator polityk parsuje zapytania i odpowiedzi HTTP, dostarczając unikalnej możliwości dwukierunkowej, pełnej inspekcji ruchu do aplikacji – zarówno dane jak i protokół. Używając zaawansowanych silników statystycznych i heurystycznych, generator polityk jest w stanie odróżnić ataki od prawidłowego ruchu. Generator polityk może być również uruchomiony w trybie akceptowania aktualizacji aplikacji. Podczas parsowania ruchu jest w stanie wykryć zmiany w aplikacji i automatycznie uaktualnić politykę, bez konieczności interwencji administratora.

## Ochrona „Out-of-the-Box”

BIG-IP ASM jest wyposażony w zestaw wbudowanych polityk dotyczących najpopularniejszych aplikacji webowych takich jak Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials i Microsoft Office SharePoint. Dodatkowo, BIG-IP ASM, zawiera polityki szybkiego wdrożenia, które są w stanie ochronić dowolną aplikację. Polityki te są najczęściej punktem startowym dla bardziej zaawansowanej konfiguracji bazującej na uczeniu się ruchu przepływającego przez urządzenie, oraz specyficznych potrzebach klienta.

## Wymuszanie

BIG-IP ASM potrafi ochronić dowolny parametr przed manipulacją po stronie klienta. Jest w stanie sprawdzać również parametry logowania i zapobiegać atakom typu „forceful browsing” i zmianom przepływu informacji w aplikacji. BIG-IP ASM chroni również przeciw 10 najpopularniejszym zagrożeniom OWASP oraz przed atakami zero-day na aplikacje webowe.

## Zintegrowany XML Firewall

BIG-IP ASM dostarcza również możliwość sprawdzania i filtrowania XML. Umożliwia sprawdzanie schematu, chroni przed najczęstszymi atakami i zapewnia ochronę przed atakami typu denial-of-service na parser XML'a.

## Ochrona danych i maskowanie

BIG-IP ASM zapobiega wyciekowi wrażliwych informacji (numery kart kredytowych, PESEL, jakiegokolwiek inne krytyczne dane) poprzez ich maskowanie. Dodatkowo BIG-IP ASM może ukrywać strony z komunikatami błędów serwera oraz aplikacji, uniemożliwiając w ten sposób hakerom zebranie informacji o architekturze potencjalnego celu.

## Integracja z WhiteHat Sentinel

WhiteHat Security oferuje unikalne rozwiązanie wykrywania słabości w aplikacjach webowych. Poprzez integrację z BIG-IP ASM, WhiteHat Sentinel może wygenerować reguły dla ASMA, które po zaimplementowaniu dokładnie zapewniają ochronę przed wykrytymi słabościami.

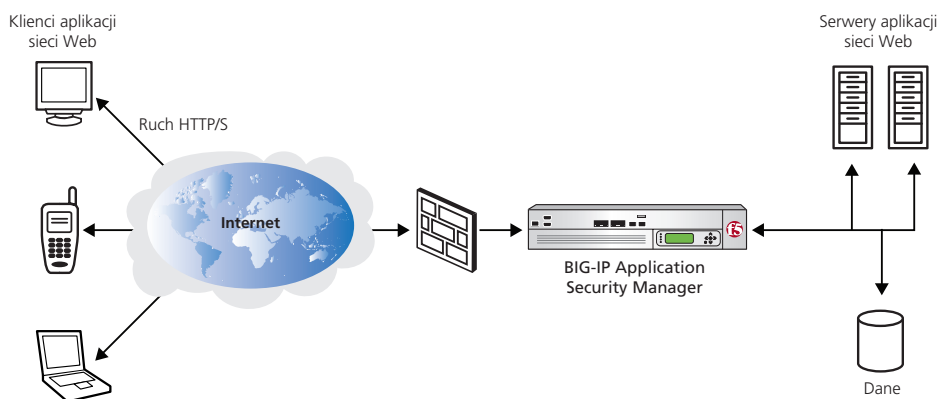
BIG-IP ASM zawiera wbudowane zatwierdzone zasady dotyczące zabezpieczeń aplikacji, które nie wymagają żadnej konfiguracji i oferują gotową ochronę aplikacji o decydującym znaczeniu z punktu widzenia firmy.

<input type="checkbox"/>	Name	Active Security Policy	Enforcement Mode	Logging Profile	State
<input type="checkbox"/>	OWA	A M OWA_default	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	Oracle_11i	A M Oracle_11i	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	PeopleSoft_Portal	A PeopleSoft_Portal_default	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	SharePoint	A SharePoint_Template	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	www.mycompany.com	A www.mycompany.com_default	Blocking	Log all requests	VS1 Enabled

BIG-IP ASM oferuje kompleksową ochronę aplikacji sieci Web.

## Uaktualnienia sygnatur

Nowe sygnatury na nowe ataki są konieczne do prawidłowego funkcjonowania systemu i zapewnienia odpowiedniego poziomu bezpieczeństwa. BIG-IP ASM codziennie odpytuje serwis uaktualnień F5 oraz automatycznie ściąga i instaluje nowe sygnatury bez konieczności ręcznej interwencji.



## Zabezpieczenie protokołów SMTP i FTP

BIG-IP ASM ułatwia także zarządzalność farmą serwerów FTP. BIG-IP ASM sprawdza protokół FTP, eliminując możliwość ataku brute-force, posiada możliwość zdefiniowania dozwolonych komend FTP oraz może wymuszać limit długości komend dla sesji aktywnych/pasywnych. W zakresie protokołu SMTP, BIG-IP ASM wprowadza dodatkową ochronę na brzegu sieci. Wspierane są mechanizmy greylistingu (aby zapobiec wiadomościom SPAM), wymuszania zgodności protokołu SMTP, blokowania wybranych koment SMTP oraz ograniczania ataków typu directory-harvesting. Mechanizmy limitowania pasma pomagają walczyć z atakami typu denial-of-service.

## Wszzechstronna ochrona aplikacji

BIG-IP ASM działa na F5 TMOS. Jest on inteligentnym, modularnym i wysoko wydajnym systemem operacyjnym. Dostarcza on wgląd, elastyczność i kontrolę niezbędną przy ochronie aplikacji webowych.

### TMOS dostarcza:

- Terminacja połączeń SSL
- Caching
- Kompresja
- Możliwość manipulacji zawartości pakietu w locie
- Optymalizację TCP/IP
- Wsparcie dla IPv6
- Filtrowanie adresów/portów
- Wsparcie dla VLAN

### BIG-IP ASM chroni przed atakami typu:

- Cross-site scripting
- SQL injection
- Parameter tampering
- Wyciekowi istotnych informacji
- Przejmowaniu sesji
- Manipulacją plikami cookie
- Kodowanie
- Broken access control

- Forceful browsing
- Manipulacja ukrytymi wartościami
- Request smuggling
- XML bombs/DOS

### Dodatkowe bezpieczeństwo serwisów sieciowych – BIG-IP ASM zawiera także:

- SSL akcelerator
- Stateful firewall warstwy 3-4
- Przezroczyste i nieprzezroczyste odwrócone proxy
- Możliwość zarządzania kluczami i failover
- Możliwość terminacji sesji SSL i ich ponowne szyfrowanie
- Segmentacje VLAN
- Ochronę przed atakami denial-of-service
- Wsparcie dla certyfikatów klienta
- Autentykację klienta w LDAP/RADIUS
- Dedykowany port zarządzający

## Specyfikacja platform sprzętowych

BIG-IP ASM jest dostępny jako moduł programowy na urządzeniach Viprion, 8900, 6900, 3900, 3600 lub jako rozwiązanie wolnostojące na platformach 8900, 6900, 3900, 3600. Rozwiązanie wolnostojące zawiera dodatkowo licencje: IPv6, zaawansowanej autentykacji klienta, maksimum SSL TPS, moduł rate-shaping, caching i kompresję 5 Mbitów.



VIPRION Chassis



8900 Series



6900 Series



3900 Series



3600 Series