ALEF

Trust the Strong

Big-IP ASM | Chráňte sa pred útokmi na webe

OBSAH DOKUMENTU

Charakteristika

S neustálym rastom prenosu dát webových aplikácií je stále väčšie množstvo citlivých údajov vystavené riziku odcudzenia a rizikám spojeným so zneužitím bezpečnostných chýb softvéru a viacvrstvovými útokmi. Chráňte si svoju organizáciu a jej povesť zachovaním dôvernosti, dostupnosti a rýchlej odozvy aplikácií, ktoré sú rozhodujúce pre vaše podnikanie. **F5 BIG-IP® Application Security Manager™ (ASM)** je flexibilný web aplikačný firewall pre webové aplikácie, ktorý chráni webové aplikácie v tradičnom, virtuálnom a privátnom prostredí služieb typu cloud. BIG-IP ASM zabezpečuje bezkonkurenčnú ochranu pre webové aplikácie a webové stránky, chráni prevádzkované aplikácie pred zneužitím existujúcich chýb softvéru a umožňuje zaistiť súlad s hlavnými legislatívnymi normami – a to všetko na platforme, ktorá konsoliduje poskytovanie aplikácií s bránou firewall dátového centra a riadením prístupu do siete a k aplikáciám.

Hlavné prínosy

Garancia zabezpečenia a dostupnosti aplikácií

Získajte komplexnú geolokačnú ochranu pred útokmi na vrstve 7 formou DDoS (distribuovaný útok zahltením servera služby), vložením kódu do databázy SQL injection a útokmi z OWASP Top Ten rebríčka a zabezpečte si najnovšie interaktívne AJAX aplikácie a JSON notifikácie.

Nižšie náklady a podpora pre zaistenie súladu s normami

Zaistite súlad s požiadavkami bezpečnostných noriem so zabudovanou aplikačnou ochranou.

Politiky zabezpečenia aplikácií out-of-the-box

Zabezpečte si ochranu so vstavanými politikami pre rýchle nasadenie a s minimálnou konfiguráciou.

Vyššia miera zabezpečenia a výkonu aplikácií

Aplikujte rozšírené zabezpečenie aplikácií, čím dosiahnete zvýšenie výkonu s lepšou odozvou aplikácií pri vyššej efektívnosti nákladov.

Pružné nasadzovanie a začlenenie externej inteligencie

Zamerajte sa na rýchly vývoj aplikácií a flexibilné nasadenie vo virtuálnom a cloudovom prostredí a zároveň implementujte externú inteligenciu na zaistenie aplikácií pred IP hrozbami.

Komplexná ochrana pred útokmi

Udržiavanie kroku s veľkým množstvom bezpečnostných útokov a ochranných opatrení môže byť pre správcov a bezpečnostné tímy výzvou. Preťaženie informáciami a stále sofistikovanejšie útoky pridávajú na náročnosti. BIG-IP ASM poskytuje komplexnú a nákladovo efektívnu ochranu pred útokmi pre najnovšie interaktívne aplikácie pre Web 2.0 a súčasne uľahčuje prácu správcom.

Zabezpečenie pre najnovšie interaktívne webové aplikácie

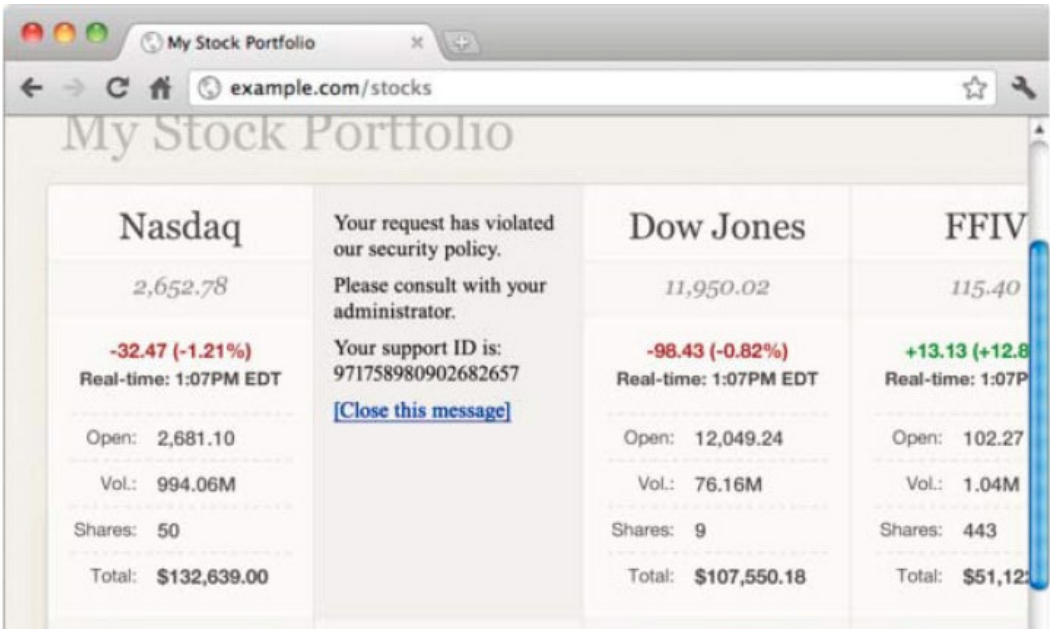
Mnohé z najnovších aplikácií pre Web 2.0 umožňujú používať Asynchronous JavaScript and XML (AJAX) na vytváranie interaktívnych webových aplikácií. Pri použití AJAX sú dáta posielané z aplikácie s notifikáciami JavaScript Object Notation (JSON) na server a z neho a zobrazené informácie sú aktualizované bez obnovenia stránky. Zle napísaný kód umožňuje útočníkom upraviť aplikáciu, spustiť XSS alebo zaútočiť prevzatím kontroly aplikácie a ohroziť bezpečnosť osobných údajov.

BIG-IP ASM zabezpečuje najnovšie aplikácie pre Web 2.0 a chráni cenné informácie pred zneužitím v dôsledku existencie bezpečnostných chýb softvéru. Vykreslí jedinečnú blokovaciu stránku s pomocným ID pre oddelenie IT, ktorá informuje používateľa o porušení politiky pre miniaplikácie AJAX. BIG-IP ASM vynucuje prísne pravidlá týkajúce sa údajov v notifikáciách JSON a chráni aplikácie pred najnovšími JSON webovými hrozbami.

Rozšírené vynucovanie bezpečnostných pravidiel

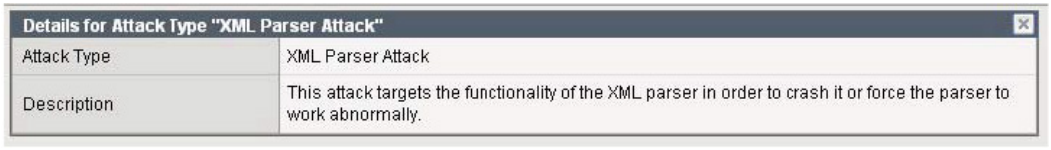
BIG-IP ASM dokáže zabezpečiť akýkoľvek parameter pred manipuláciou na strane klienta a overiť prihlasovacie parametre a správnu postupnosť krokov v rámci aplikácie s cieľom zabrániť útokom typu forcefull browsing resp. zneužitiu logických chýb aplikácie.
Útoky typu HTTP parameter pollution (HPP) sú reprezentované formuláciou nevalidnej požiadavky formou modifikácie URL v kombinácii s nevalidnými parametrami za účelom obídenie zabezpečenia aplikácií. BIG-IP ASM rozpozná tieto útoky a zablokujte tieto požiadavky, čím vytvára granulárnu ochranu pred útokmi.

Podľa správy 2012 Verizon Data Breach Investigations Report boli v 54 % prípadov úniku údajov vo veľkých organizáciách použité webové aplikácie ako vstupná brána pre realizáciu útoku.



Keď dôjde k porušeniu politiky, BIG-IP ASM vygeneruje jedinečný prehľad o blokovaní pre miniaplikácie AJAX a ochráni údajové časti JSON.

Komplexná ochrana pred útokmi



Details for Attack Type "XML Parser Attack"	
Attack Type	XML Parser Attack
Description	This attack targets the functionality of the XML parser in order to crash it or force the parser to work abnormally.

Expertný systém brány BIG-IP ASM poskytuje podrobný opis zistených útokov.

BIG-IP ASM zároveň chráni na vrstve 7 pred útokmi DoS, databázovým SQL injection útokom, cross-site scripting (XSS), útokmi brute force a day-zero útokmi na webové aplikácie. Okrem toho BIG-IP ASM chráni aplikácie pred bezpečnostnými rizikami OWASP Top Ten rebríčka najčastejších typov útokov a hrozieb na webové aplikácie. Napríklad útok Cross Site Request Forgery, ktorý je na zozname OWASP Top Five, si vynúti z prehľadávača obete odoslať utajenú platnú požiadavku na dôveryhodné webové stránky, na ktorých má obeť vytvorenú platnú reláciu. Útočníci vykonávajú podvodné transakcie, ako sú prevody finančných prostriedkov, a pre obete je ťažké dokázať, že požiadavku nevykonali. BIG-IP ASM eliminuje tieto útoky a chráni aplikácie pomocou explicitného potvrdenia transakcie formou zobrazeného checkboxu.

Expertný systém pre škálu rôznych typov útokov

S rastúcim počtom a zložitosťou hrozieb poskytuje integrovaný a komplexný expertný systém pre útoky v BIG-IP ASM okamžitý, podrobný opis útoku a tiež okamžitú viditeľnosť zvolenej metódy na elimináciu konkrétneho rizika, ktoré BIG-IP ASM aplikovalo na detekciu a prevenciu útokov. Expertný systém pre útoky preklenuje medzeru medzi sieťou a aplikačným tímom a vzdeláva správcu v oblasti zabezpečenia aplikácií.

Prevencia zberu webových údajov (Web scraping)

BIG-IP ASM pomáha chrániť vašu značku tým, že chráni vaše webové stránky pred útokmi so zberom webových údajov (web scraping), ktoré kopírujú a následne neautorizovane využívajú vaše cenné duševné vlastníctvo a informácie. Keďže BIG-IP ASM dokáže rozlíšiť človeka od robota za prehliadačom, chráni pred automatizovanými žiadosťami o získanie údajov. Politiky pre webové aplikácie dokážu rozpoznať nárast objemu požiadaviek a upozornia systém BIG-IP ASM, aby preskúmal, či sú požiadavky platné. Známe adresy IP schválené pre zber webových údajov môžu byť vložené do zoznamu povolených položiek — whitelistov s cieľom povoliť zber údajov.

Identifikácia relácie a vynucovanie bezpečnostných politík

Pri vytvorení relácie zaisťuje BIG-IP ASM hĺbkové blokovanie plus umožňuje lepšie porozumieť mechanizmu útoku tým, že počas relácie priradí odchýlkam zo štandardnej procedúry aplikačné používateľské meno. Správcovia BIG-IP ASM majú možnosť jednoznačne identifikovať a odlíšiť, že útok databázy SQL injection na webových stránkach vykonal používateľ s menom „Bob_Smith“.

Integrovaný XML firewall

BIG-IP ASM používa filtrovacie a overovacie funkcie pre XML podľa konkrétnej aplikácie, ktoré zabezpečujú, že kód XML vkladaný do webových aplikácií je správne štruktúrovaný. Robí overovanie schém, eliminuje typické XML útoky a posktuje prevenciu DoS útoku parserom XML.

DataGuard a maskovanie

BIG-IP ASM zabraňuje úniku citlivých údajov (ako sú čísla kreditných kariet, rodné čísla a iné) tým, že odstraňuje údaje a maskuje informácie. BIG-IP ASM ďalej skrýva chybové stránky a informácie o chybách aplikácií a znemožňuje hackerom identifikovať architektúru riešenia a spustiť cielený útok na danú architektúru.

BIG-IP ASM poskytuje komplexnú ochranu pre webové aplikácie.

—

Vykazovanie PCI

Pri náraste objemu útokov pozorujú mnohí sieťoví technici tisíce odchýliek od normálu a v záplave informácií sa im nemusí podariť zistiť, ktoré z nich sú spojené s konkrétnym incidentom. BIG-IP ASM umožňuje technikom korelovať tisíce udalostí a vidieť „incidenty“ v skupine, ktoré sú prepojené so spoločným pravidlom alebo spoločným kritériom. Napríklad niekoľko útokov z rovnakej adresy IP zdroja je spojených s jediným incidentom pre lepšiu viditeľnosť a správu.

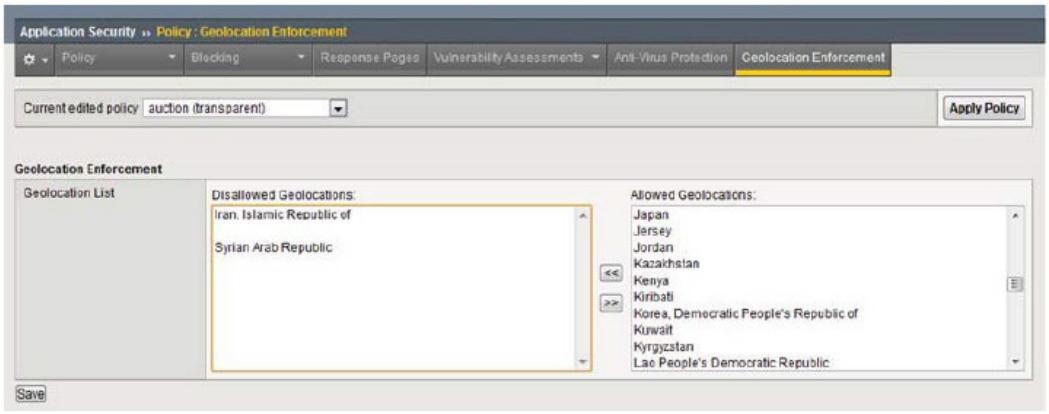
Komplexná ochrana pred útokmi

Aktualizácia signatúr v reálnom čase

Nové signatúry popisujúce nové typy útokov sú často nevyhnutné na zabezpečenie najaktuálnejšej ochrany. BIG-IP ASM každodenne posiela požiadavky do F5 a automaticky preberá a aplikuje nové signatúry.

Geolokačné blokovanie

S narastajúcimi útokmi z mnohých rôznych miest planéty BIG-IP ASM dovoľuje blokovať útoky podľa krajín, regiónov alebo štátov na základe geolokačných údajov. BIG-IP ASM umožňuje správcom ľahko vybrať povolené alebo zakázané geolokácie pre vynucovanie striktnejšej bezpečnostnej politiky pre adekvátnu ochranu pred útokmi.



Geolokačné blokovanie je jednoducho nastaviteľné výberom krajín alebo regiónov pre vynucovanie.

Podpora pre antivírusový bezpečnostný protokol

Najrozšírenejší bezpečnostný protokol pre odosielanie a prijímanie súborov na kontrolu prítomnosti vírusov je Internet Content Adaptation Protocol (ICAP). BIG-IP ASM odstráni nahrané súbory SOAP a SMTP z požiadavky HTTP a pošle ich na antivírusový server cez ICAP. Ak je súbor čistý, antivírusový server odpovie schválením požiadavky. Ak súbor nie je čistý, BIG-IP ASM zablokuje požiadavku, aby chránil sieť pred preniknutím vírusu.

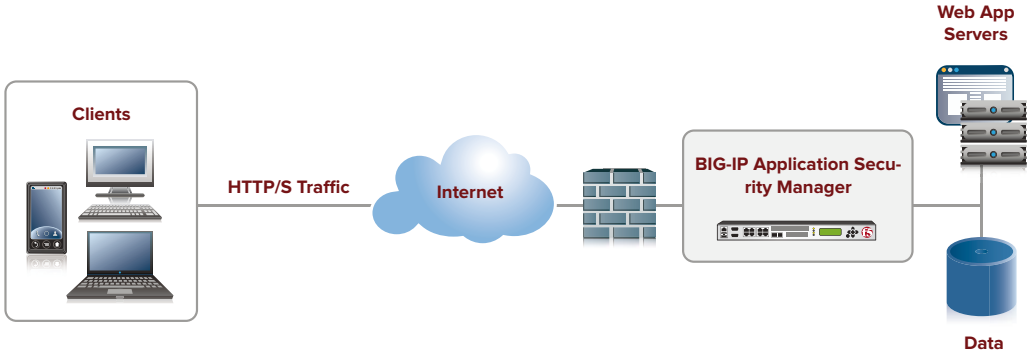
Zabezpečenie pre SMTP a FTP

BIG-IP ASM uľahčuje správu serverových fariem FTP. Overuje FTP protokol, obmedzuje brute force útoky a zároveň umožňuje používať zoznam povolených príkazov FTP (whitelisty). Navyše dokáže vynucovať obmedzenia dĺžky príkazov a pasívne/aktívne pripojenia.

V prípade SMTP robí BIG-IP ASM dodatočné bezpečnostné kontroly po obvode. Podporuje aj zoznamy dočasne zakázaných položiek eliminujúce nevyžiadanú poštu, vynucuje protokol SMTP, zakazuje nebezpečné príkazy SMTP a eliminuje útoky na získavanie údajov z adresárov – directory harvesting útoky. Funkcia brány BIG-IP ASM na nastavenie limitov priepustnosti rate-limiting pomáha v boji proti útokom DoS.

Jednoduchosť pri zabezpečení webových služieb

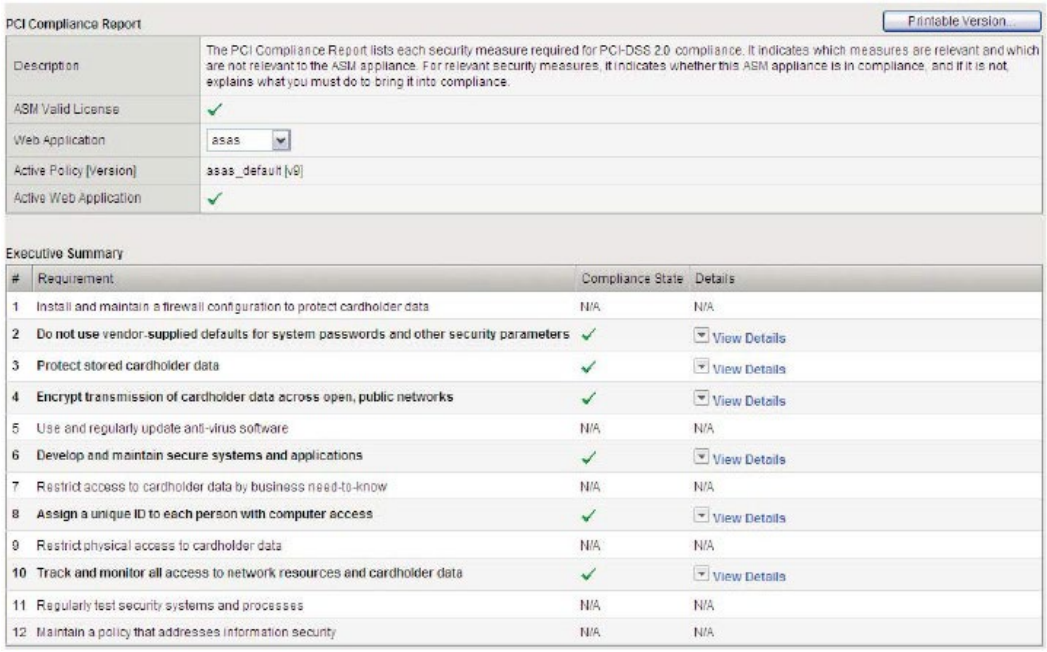
BIG-IP ASM odbremeňuje zaťaženie pri šifrovaní a dešifrovaní webových služieb a podpisovaní a overovaní digitálnych podpisov. Umožňuje ľahko spravovať a konfigurovať tieto funkcie centralizovane priamo v systéme BIG-IP, vrátane možnosti šifrovania alebo dešifrovania správ SOAP a overenia podpisov bez nutnosti meniť kód aplikácie.



Vstavaná podpora pre súlad s legislatívnymi normami

Brána firewall pre dátové centrum

V dôsledku neustáleho rastu viacvrstvových útokov, ako sú sieťové DDoS a DDoS na vrstve 7, databázové SQL injection, útoky cross-site scripting a iné, narastá potreba na konsolidáciu siete a vyvstáva potreba nasadenia web aplikačného firewallu. BIG-IP LTM a BIG-IP ASM pokrývajú spektrum hrozieb od vrstvy 3 po vrstvu 7, pričom konsolidujú ochranu pred útokmi do jednej unifikovanej bezpečnostnej architektúry. BIG-IP Global Traffic Manager (GTM) prináša funkcie brány DNS firewallu, ktoré pomáhajú chrániť vašu infraštruktúru DNS. BIG-IP Access Policy Manager (APM) umožňuje aplikovať kontextovú bezpečnosť pripájania užívateľov a aplikáciu adekvátnej bezpečnostnej politiky, čím súčasne chráni sieť a aplikácie pred nepovoleným prístupom. Systém BIG-IP ako celok prináša certifikovanú bránu aplikačného firewallu, bránu DNS firewallu a služby zabezpečenia kontroly prístupu s hĺbkovými kontrolami a eliminaciou hrozieb pre dynamickú ochranu dátového centra.



PCI Compliance Report — Printable Version

Description	The PCI Compliance Report lists each security measure required for PCI-DSS 2.0 compliance. It indicates which measures are relevant and which are not relevant to the ASM appliance. For relevant security measures, it indicates whether this ASM appliance is in compliance, and if it is not, explains what you must do to bring it into compliance.
ASM Valid License	✓
Web Application	asas
Active Policy [Version]	asas_default [v9]
Active Web Application	✓

Executive Summary

#	Requirement	Compliance State	Details
1	Install and maintain a firewall configuration to protect cardholder data	N/A	N/A
2	Do not use vendor-supplied defaults for system passwords and other security parameters	✓	View Details
3	Protect stored cardholder data	✓	View Details
4	Encrypt transmission of cardholder data across open, public networks	✓	View Details
5	Use and regularly update anti-virus software	N/A	N/A
6	Develop and maintain secure systems and applications	✓	View Details
7	Restrict access to cardholder data by business need-to-know	N/A	N/A
8	Assign a unique ID to each person with computer access	✓	View Details
9	Restrict physical access to cardholder data	N/A	N/A
10	Track and monitor all access to network resources and cardholder data	✓	View Details
11	Regularly test security systems and processes	N/A	N/A
12	Maintain a policy that addresses information security	N/A	N/A

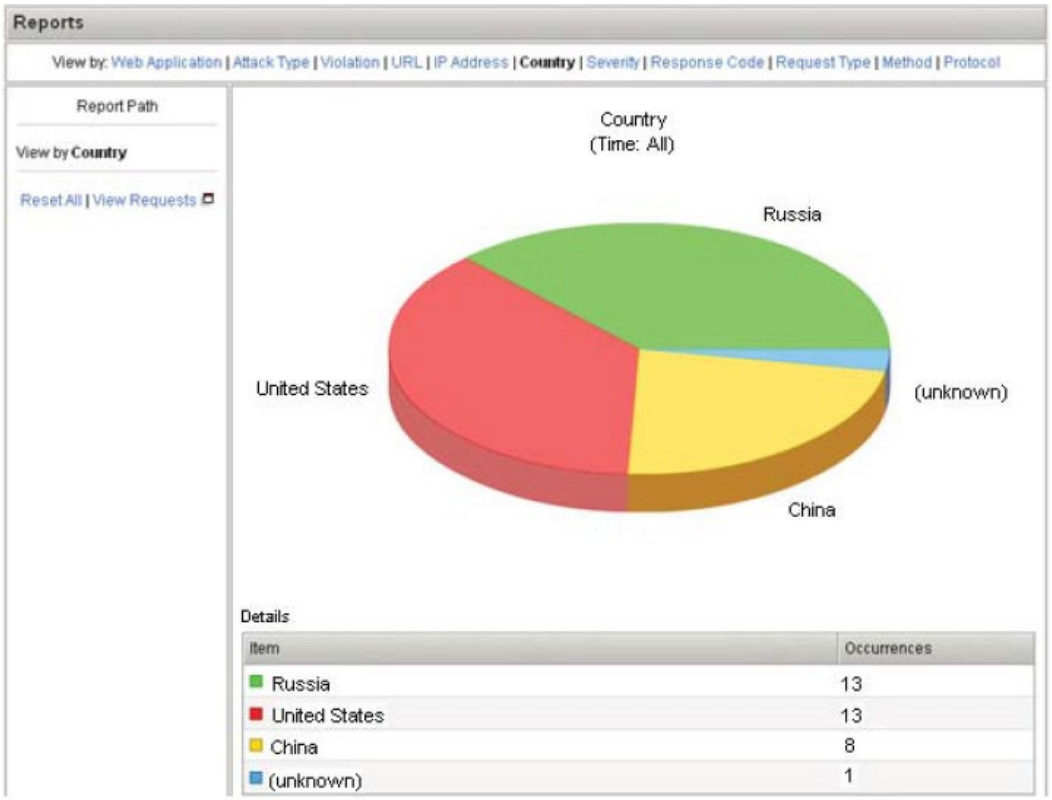
Rozšírená, vstavaná ochrana zabezpečenia a audit na diaľku pomôžu vašej organizácii zaistiť súlad s požiadavkami priemyselných bezpečnostných noriem, vrátane priemyselnej normy o ochrane údajov o platobných kartách (PCI DSS), HIPAA, Basel II a SOX za prijateľnú cenu a bez potreby vlastniť viacero zariadení, meniť aplikácie či prepisovať kód. BIG-IP ASM hlási doposiaľ neznáme hrozby, ako sú útoky zahltením servera na vrstve 7 (DoS) a databázové SQL injection útoky a eliminuje hrozby pre webové aplikácie s cieľom chrániť organizáciu pred únikom senzitívnych údajov. Komfortný reporting dostupný cez grafické rozhranie GUI obsahuje prehľadné možnosti, ktoré je možné detailne skúmať cez drill-down voľbu na jedno kliknutie.

Vykazovanie PCI

Pomocou funkcie „vykazovanie PCI“ vytvára BIG-IP ASM zoznam bezpečnostných opatrení vyžadovaných podľa PCI DSS 2.0, určuje, či sú splnené požiadavky a ďalej určuje kroky potrebné na zaistenie súladu.

Geolokačné vykazovanie

Okrem typu útoku, porušenia, URL, adresy IP, závažnosti a iných údajov informuje funkcia „geolokačné vykazovanie“ aj o krajine pôvodu hrozieb. Umožňuje tiež naplánovať automatické odosielanie aktuálnych prehľadov na určenú e-mailovú adresu.



Riadenie politík

Prehľadný formát pre audit na diaľku

BIG-IP ASM uľahčuje zaistenie súladu s bezpečnostnými požiadavkami a šetrí drahocenný čas pracovníkov IT exportovaním politík vo formáte, ktorý je zrozumiteľný človeku. Uhladený, zrozumiteľný formát súborov XML umožňuje audítorom zobraziť politiky off site. Audítori pracujúci na diaľku majú možnosť zobraziť, vybrať, skontrolovať a testovať politiky bez pomoci správcu zabezpečenia webových aplikácií.

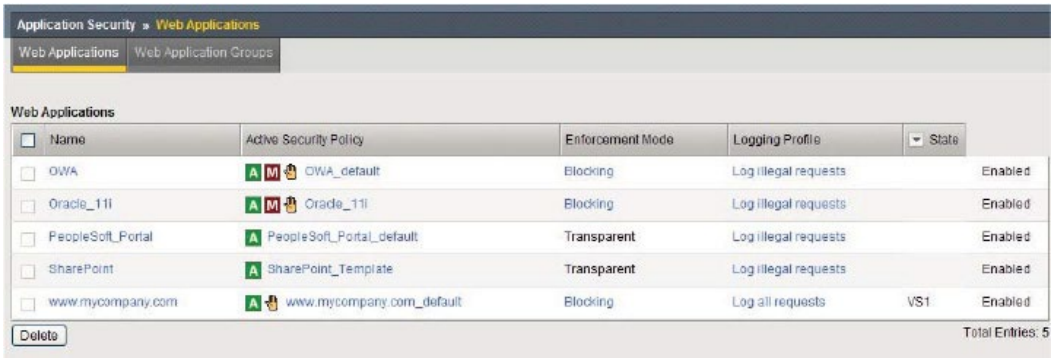
Webové stránky z titulu dynamického obsahu sú rôznorodé, komplexné a neustále sa menia, čo si vyžaduje politiky so stovkami, ak nie tisícmi jasných a presných pravidiel. BIG-IP ASM pomáha bezpečnostným tímom zvládať tieto zmeny pri zachovaní krehkej rovnováhy medzi zaistením najprísnejších možných bezpečnostných kontrol a umožnením prístupu oprávneným používateľom.

Podľa správy 2012 Verizon Data Breach Investigations Report boli v 54 percentách prípadov úniku údajov vo veľkých organizáciách použité webové aplikácie ako vstupná brána pre realizáciu útoku.

Okamžitá ochrana bez potreby konfigurácie – out-of-the-box

V dôsledku neustáleho rastu viacvrstvových útokov, ako sú sieťové DDoS a DDoS na vrstve 7, databázové SQL injection, útoky cross-site scripting a iné, narastá potreba na konsolidáciu siete a vyvstáva potreba nasadenia web aplikačného firewallu. BIG-IP LTM a BIG-IP ASM pokrývajú spektrum hrozieb od vrstvy 3 po vrstvu 7, pričom konsolidujú ochranu pred útokmi do jednej unifikovanej bezpečnostnej architektúry. BIG-IP Global Traffic Manager (GTM) prináša funkcie brány DNS firewallu, ktoré pomáhajú chrániť vašu infraštruktúru DNS. BIG-IP Access Policy Manager (APM) umožňuje aplikovať kontextovú bezpečnosť pripájania užívateľov a aplikáciu adekvátnej bezpečnostnej politiky, čím súčasne chráni sieť a aplikácie pred nepovoleným prístupom. Systém BIG-IP ako celok prináša certifikovanú bránu aplikačného a firewallu, bránu DNS firewallu a služby zabezpečenia kontroly prístupu s hĺbkovými kontrolami a elimináciou hrozieb pre dynamickú ochranu dátového centra.

Riadenie politík



Testačný mód – staging

Staging funkcia sprehľadňuje aktualizované politiky pre testovanie v živom prostredí bez zníženia aktuálnej úrovne ochrany. BIG-IP ASM uľahčuje prípravu politík pomocou podpisov útokov, typov súborov, adries URL a iných parametrov a pomáha určiť, či pred vynucovaním politiky je potrebné urobiť zmeny. Politiku môžete prepracovať a opakovane testovať, až kým s ňou nebudete úplne spokojní, a kým politika nebude pripravená na zavedenie do produkčného prostredia.

Integrácia pravidiel iRules

Môžete navrhnúť vami definované iRules®, ktoré sa aktivujú pri výskyte definovanej udalosti BIG-IP ASM. Napríklad politika pre blokovanie stránky môže byť použitá na ochranu niekoľkých webových stránok pomocou pravidla iRule, ktoré pri zistení neautorizovaného zberu webových údajov botom otvorí prispôsobenú blokovaciu stránku pre konkrétnu webovú doménu. Mnohé udalosti BIG-IP ASM môžu byť prispôsobené vášmu jedinečnému prostrediu aplikovaním vhodne definovanej iRule procedúry.

Nástroj na vytváranie politík prenosu dát v reálnom čase

V srdci BIG-IP ASM je dynamický nástroj na vytváranie politík, ktorý je zodpovedný za automatické učenie a vytváranie politík zabezpečenia. Automaticky vytvára a spravuje politiky zabezpečenia okolo novo zistených chýb zabezpečenia a rýchlo a pružne zavádza obchodné procesy bez ručného zasahovania. Nástroj na vytváranie politík analyzuje pri prenose dát cez BIG-IP ASM požiadavky a odpovede a kontroluje obojsmerný tok všetkých prenosov klienta a aplikácie – dát aj protokolu. Rozšírené štatistické a heuristické jadro umožňuje nástroju odfiltrovať útoky a nezvyčajné prenosy. Nástroj na vytváranie politík môže byť spustený aj v režime, v ktorom si je vedomý aktualizácií lokalít. Na základe analýzy odpovedí a požiadaviek dokáže zistiť zmeny na lokalitách a podľa toho automaticky aktualizuje politiku bez zásahu používateľa.

iApps pre prednastavené politiky

F5 iApps™ poskytuje pracovníkom zodpovedným za aplikácie, zabezpečenie, sieť, systém a prevádzku rámec na zjednotenie, zjednodušenie a kontrolu sietí ADN (Application Delivery Network) s kontextovým náhľadom a rozšírenou štatistikou aplikačných služieb na podporu podnikania. iApps podporuje aplikácie so zabezpečením BIG-IP ASM pomocou prednastavených politík pre jednoducho použiteľné a flexibilné šablóny pre nasadenie aplikačných služieb, čím zvyšuje pružnosť a efektivitu IT.

Rýchle vytváranie politík a užitočné rady

Užitočné rady pri konfigurácii a zavádzaní politík zabezpečenia aplikácií v BIG-IP ASM pomáhajú vytvárať silnejšie politiky, lepšie chrániť aplikácie a zaistiť silnejšiu reakciu na rôzne hrozby. Používateľské rozhranie napríklad obsahuje zoznam užitočných prepojení v podobe rýchlych prepojení (Quick Links), ktoré pomáhajú zvyšovať produktivitu a presnosť pri navrhovaní politiky zabezpečenia. Zoznam úloh (To Do list) okrem toho zobrazuje odporúčania na optimalizáciu politík BIG-IP ASM.

Viditeľnosť aplikácií a reporting

BIG-IP ASM sleduje a hlási najviac žiadané identifikátory URI a každý identifikátor URI s latenciou servera. Zviditeľňuje pomalé serverové skripty a odstraňuje problémy s kódom na serveri, ktoré spôsobujú latenciu.

BIG-IP ASM sleduje stránky s najväčším počtom prístupov podľa webovej aplikácie, za poslednú hodinu, posledný deň a posledný týždeň. Pre tieto stránky poskytuje priemerné TPS a priemerné trvanie latencie. BIG-IP ASM navyše poskytuje pre každú webovú aplikáciu zoznam adries IP zdroja s najväčším počtom prístupov spolu s TPS a priepustnosťou pre každú adresu IP. Tieto sledovacie funkcie poskytujú správcom prehľad o tom ako sa pristupuje k aplikácii a s akou odozvou aplikácia reaguje.
—

Integrácia pre flexibilnosť a adaptabilitu

Schopnosť reagovať na časté zmeny metód útoku a vášho počítačového prostredia je kľúčovou zložkou zabezpečenia webových aplikácií. Možnosť integrácie s produktmi tretích strán robí z BIG-IP ASM dynamické a prispôsobiteľné bezpečnostné riešenie.

Podrobné hodnotenie zraniteľnosti a ochrana aplikácií

BIG-IP ASM je možné integrovať s najrozšírenejšími skenermi webových aplikácií a nástrojmi na hodnotenie zraniteľnosti s cieľom poskytovať jedinečnú službu na hodnotenie zraniteľnosti, ktorá spája automatizované nástroje spoločnosti F5 s odbornými vedomosťami špecializovaných, vysoko kvalifikovaných odborníkov na zabezpečenie aplikácií. Rozšírená integrácia BIG-IP ASM umožňuje ezpečnostným službám tretích strán prehľadávať webové aplikácie a vytvárať politiky BIG-IP ASM, ktoré sú špeciálne zamerané na slabé miesta objavené v aplikácii. BIG-IP ASM umožňuje správcom spravovať hodnotenia zraniteľnosti a eliminovať hrozby z jedného miesta.

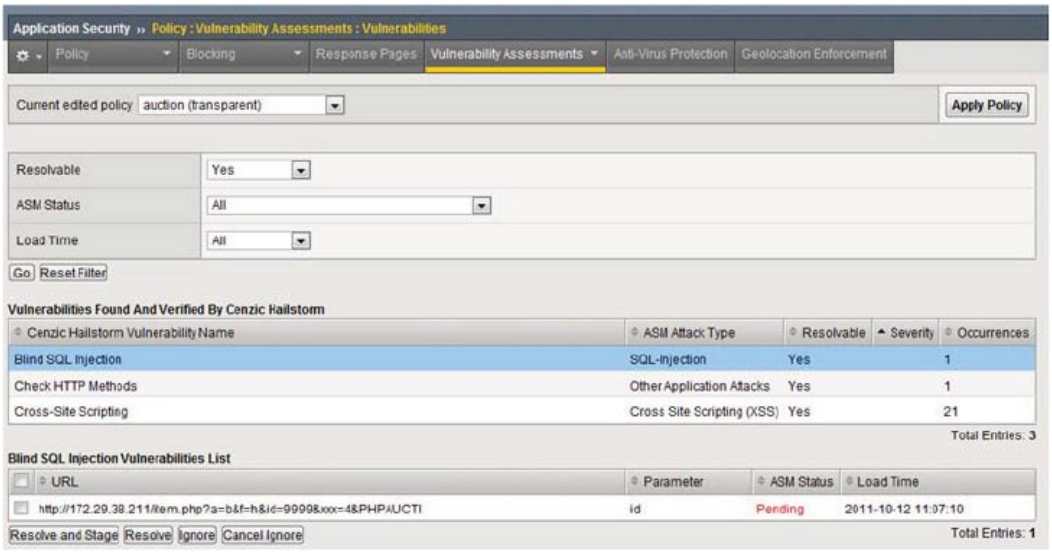
Jednoduchým odhalením slabých miest, vytvorením, prípravou a zavedením politík a opakovaným testovaním prehľadávania aplikácií vytvoríte trvalú ochranu pred slabými miestami a riešenie na vynucovanie politiky. Výsledkom je overené a funkčné hodnotenie zraniteľnosti s istotou ochrany pred slabými miestami počas alebo po skončení cyklu vývoja softvéru (SDLC). Tento proces zaisťuje takmer okamžitú reakciu na elimináciu hrozby a chráni vašu aplikáciu, kým vaši vývojári opravia zraniteľný kód.

Nad rámec aktuálnej politiky, ako je politika rýchleho nasadenia alebo politika služby SharePoint, môžete tiež jednoducho navrstviť politiku na báze zraniteľnosti (získanú z integrácie skenera F5) pre vytvorenie politík viacnásobného nasadenia. Takto sa vnáša istota, že bez ohľadu na to, ako správca vytvorí politiky, ďalšie prehľadávanie hodnotenia zraniteľnosti umožňuje systému BIG-IP ASM navrstviť politiku na báze prehľadávania nad rámec existujúcej politiky pre vrstvenú ochranu pred útokmi.

Integrácia štyroch prehľadávacích služieb umožňuje správcom brány BIG-IP ASM importovať identifikované slabé miesta do BIG-IP ASM na vytvorenie politiky. Ide o tieto služby:

- Cenzic Hailstorm (používateľské rozhranie BIG-IP ASM umožňuje spustiť tri voľné prehľadávania v rámci služby Cenzic Cloud)
- IBM Rational AppScan
- QualysGuard Web Application Scanning
- WhiteHat Sentinel

Vyhľadávanie slabých miest webových aplikácií s integráciou služby Cenzic Hailstorm alebo Cenzic Cloud sa spracuje pomocou používateľského rozhrania BIG-IP ASM (pre zákazníkov služby Cenzic), alebo je dostupné ako tri voľné prehľadávania po registrácii na odber služby Cenzic Cloud. Po prehľadávaní sú slabé miesta viditeľné v používateľskom rozhraní a pripravené na sprocesovanie pre odstránenie hrozieb.



Používateľské rozhranie BIG-IP ASM s hodnotením zraniteľnosti Cenzic Hailstorm a integráciou mechanizmu eliminácie rizík BIG-IP ASM

Integrácia pre flexibilnosť a adaptabilitu

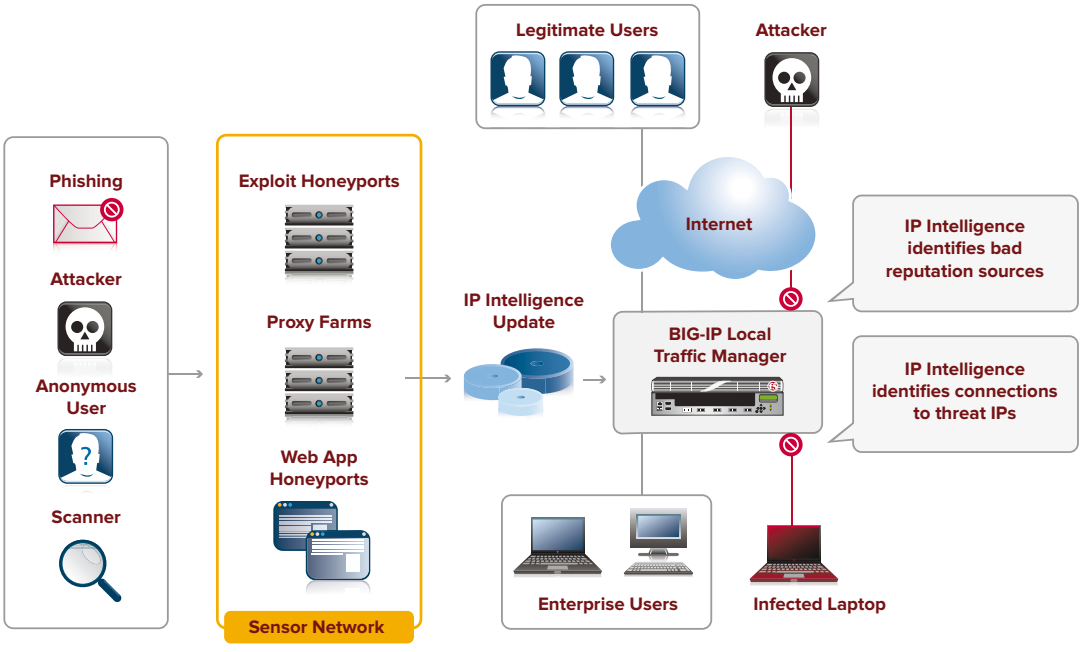
Lepšia ochrana s externou službou IP Intelligence (doplnková funkcia)

Organizácie, ktoré v dnešnej dobe poskytujú bohatý a komplexný internetový obsah používateľom bez primeranej úrovne zabezpečenia, sú vystavené značnému riziku. Zákazníci sú vystavení rôznym potenciálne škodlivým útokom z rýchlo sa meniacich adries IP. Prichádzajúce a odchádzajúce dáta internetových botov, ako je viacnásobný útok zahltením servera služby (DDoS) a činnosť škodlivého softvéru typu malware, dokážu preniknúť cez vrstvy zabezpečenia a pohlcujú cenný výpočtový výkon.

Služby F5 BIG-IP Global Delivery Intelligence Services zahŕňajú externé, inteligentné služby na zlepšenie automatizovaných rozhodnutí o poskytovaní aplikácií s lepšou inteligenciou pre riadenie adries IP a silnejším kontextovým zabezpečením. Služba IP Intelligence umožňuje identifikovaním adries IP a kategórií zabezpečenia spojených so škodlivou činnosťou používať dynamické zoznamy nebezpečných adries IP na platforme BIG-IP pre vloženie kontextu a automatizácie do rozhodnutí o blokovaní. Umožňuje nastaviť alarm alebo celý blok adries IP z určitej kategórie. Okrem toho je možné používať aj zoznam schválených adries IP.

Služba IP Intelligence pre BIG-IP Global Delivery Intelligence identifikuje adresy IP z rôznych kategórií hrozieb, vrátane nasledovných:

- **Internetové roboty** – infikované adresy IP riadené robotmi
- **Útok zahltením servera služby** – adresy IP známe útokmi DoS, DDoS, zahltením SYN
- **Zneužitie chýb systému Windows** – adresy IP známe šírením kódu na zneužitie chý operačného systému (exploity)
- **Anonymné proxy** – adresy IP používané pre anonymné služby, vrátane „onion router“ (Tor)
- **Webové útoky** – adresy IP používané na databázové SQL injection útoky, útoky na lokality sfalšovanou požiadavkou cross-site request a útoky na infraštruktúru aplikácií
- **Reputácia** – infikované adresy IP
- **Servery proxy na neoprávnené získavanie údajov** – hostitelia lokalít na neoprávnené získavanie údajov formou phishingu
- **Skenery** – sondy, prehľadávania a adresy IP používajúce hrubú silu brute force útokov



IP Intelligence zhromažďuje údaje o reputácii na použitie v riešeniach F5.

Integrácia pre flexibilnosť a adaptabilitu

Služba IP Intelligence má jedinečnú schopnosť poskytovať svoje obranné služby aj keď je používaná za sieťou na poskytovanie obsahu (Content Delivery Network) alebo inými servermi proxy. Dokáže vyhodnotiť pôvodnú skutočnú adresu IP klienta prihláseného v hlavičke X-Forwarded-For (XFF) s cieľom povoliť alebo blokovať prenos z CDN s nebezpečnými adresami IP. Iné riešenia, ako sú systémy prevencie neoprávnených vniknutí (IPS) alebo tradičné technológie brány firewall, skúmajú adresu zdroja paketov (namiesto hlavičky XFF) a nakoniec hodnotia len adresu servera proxy CDN.

Centralizovaný reporting so službou Splunk

Splunk, riešenie pre veľkorozmerné a vysokorýchlostné indexovanie a vyhľadávanie, vytvára 15 rôznych prehľadov prispôsobených pre BIG-IP ASM. Tieto prehľady poskytujú informácie o vývojových trendoch útokov a prenosov dát, dlhodobú agregáciu dát pre forenznú analýzu, zrýchlenie reakcie na incidenty a identifikáciu neočakávaných hrozieb pred samotným vystavením sa riziku.

Databázový reporting a zabezpečenie so softvérom Oracle

Integrácia brán Oracle Database Firewall a BIG-IP ASM je špičkové riešenie pre zabezpečenie webových aplikácií a databáz. Toto jedinečné riešenie zdieľa spoločné hlásenie webových pokusov o získanie prístupu k citlivým údajom, narušenie databázy či uskutočnenie útokov DoS na databáze. Izoluje používateľov so zlými úmyslami, zatiaľ čo hlásenia a upozornenia okamžite informujú o zistenom type a hrozbe útokov.

Zrýchlenie a zabezpečenie aplikácií

S aplikáciami BIG-IP ASM a BIG-IP® WebAccelerator™ spustenými spoločne na systéme BIG-IP® Local Traffic Manager™ dokážete zabezpečiť aplikácie a zároveň akcelerovať výkon. Táto efektívna, univerzálna platforma zvyšuje mieru zabezpečenia bez zníženia výkonu. Útoky sú filtrované okamžite, webové aplikácie bežia rýchlejšie a prinášajú používateľom lepší zážitok. Keďže nie je potrebné inštalovať nové zariadenia v sieti, získate kompletné riešenie pri maximálnej efektivite nákladov.

Granulárne riadenie prístupov a zabezpečenie aplikácií

BIG-IP® Access Policy Manager™ (APM) a BIG-IP ASM prinášajú služby riadenia prístupov a zabezpečenia aplikácií kombinované spoločne na systéme BIG-IP. BIG-IP APM vám umožní poskytovať používateľom kontextový prístup založený na politike a zároveň zjednodušiť autentifikáciu, autorizáciu a audit (AAA) pre webové aplikácie. BIG-IP APM je dostupný ako doplnkový modul k samostatnému zariadeniu BIG-IP ASM. BIG-IP APM-lite (s 10 voľnými používateľskými licenciami) je súčasťou každého samostatne zakúpeného riešenia BIG-IP ASM.

Zabezpečenie aplikácií vo virtuálnom prostredí a prostredí služby typu cloud

Využite plne flexibilné nasadenie s BIG-IP ASM Virtual Edition vo virtuálnych a privátnych prostrediach typu cloud. Pri presúvaní aplikácií do virtualizovaných prostredí musia správcovia zabezpečiť aplikácie pred chybami a útokmi s cieľom chrániť cenné údaje.

BIG-IP ASM s virtuálnymi a cloudovými aplikáciami vám umožní nasadiť flexibilné zabezpečenie aplikácií, navrhnúť a spravovať politiku v labe alebo produkčnom prostredí a automaticky ju simultánne synchronizovať s každou hardvérovou a virtuálnou edíciou. BIG-IP ASM umožňuje úplne virtuálnu implementáciu zabezpečenia aplikácií, ktorá sa jednoducho zavádza a podporuje zabezpečenie aplikácií v akomkoľvek prostredí.

Virtual Clustered Multiprocessing

BIG-IP ASM podporuje službu Virtual Clustered Multiprocessing (vCMP) pre cenovo efektívnu implementáciu zabezpečenia aplikácií. Systémy s podporou služieb BIG-IP a vCMP umožňujú správcom jednoducho konsolidovať niekoľko zákazníkov, skupín alebo aplikácií na jedinom zariadení. Manažérom dokážu presnejšie a vzájomne izolovane prideliť zdroje BIG-IP ASM použitím jedného harvéru BIG-IP spolu so spustením viacerých inštancií služby BIG-IP ASM.

Podľa Konzorcia pre zabezpečenie webových aplikácií (Web Application Security Consortium) obsahuje 97% webových stránok chyby zabezpečenia, ktoré vystavujú stránky bezprostrednému nebezpečenstvu útoku, a 64% týchto chýb je na strane servera. S narastajúcim počtom aplikácií presunutých na web predstavuje únik údajov z webových aplikácií skutočný problém. Ponemon Institute odhaduje, že celkové priemerné náklady spojené s únikom údajov predstavujú 214 dolárov na každý uniknutý záznam.

Zdroj: „Cost of a data breach climbs higher,“, Dr. Larry Ponemon, Ponemon Institute

Architektúra BIG-IP ASM

BIG-IP ASM beží na jedinečnom, cielene účelovom operačnom systéme TMOS® od spoločnosti F5. TMOS je inteligentný, modulárny a vysokovýkonný OS, ktorý vylepšuje každú funkciu služby BIG-IP ASM. TMOS prináša prehľad, flexibilitu a kontrolu, ktoré vám pomôžu inteligentne chrániť webové aplikácie.

Funkcie TMOS:

- Agregácia požiadaviek na pripojenie k službám OneConnect™
- Odľahčenie záťaže SSL offload
- Caching
- Kompresia
- Schopnosť manipulovať s akýmkoľvek obsahom aplikácie za chodu – on-the-fly bez ohľadu na to, či ide o prenos smerom dnu alebo von
- Optimalizácia TCP/IP
- Rozšírené regulovanie rýchlosti rate shaping a kvalita služieb QoS
- IPv6-ready Gateway™
- Filtrovanie adries IP/portov
- Podpora VLAN cez vstavaný prepínač
- Poskytovanie a správa zdrojov
- Smerovacie domény (virtualizácia)
- Autentifikácia na diaľku

Zabezpečenie

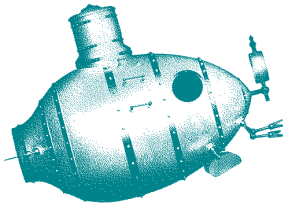
- Zobrazenie vlastných právnych oznámení
- a bannerov bezpečného prihlásenia
- Vynucovanie časových limitov relácií administrátora
- Bezpečné odhlásenie zo systému BIG-IP
- Súlad s rozšírenými požiadavkami na audit a zaznamenávanie
- Certifikáty SSL úplne izolované a zabezpečené pred čítaním a zmenou

BIG-IP ASM chráni pred rôznymi útokmi na aplikácie, vrátane nasledovných:

- AJAX/JSON web threats
- Layer 7 DoS and DDoS
- Brute force
- Cross-site scripting (XSS)
- Cross Site Request Forgery
- SQL injection
- Parameter and HPP tampering
- Sensitive information leakage
- Session highjacking
- Buffer overflows
- Cookie manipulation
- Various encoding attacks
- Broken access control
- Forceful browsing
- Hidden fields manipulation
- Request smuggling
- XML bombs/DoS

Medzi ďalšie služby zabezpečenia patria nasledovné:

- Prehľady zaistenia súladu s normou pre PCI
- Expertný systém pre útoky
- Príprava politiky
- Zjednodušené vytváranie politík a užitočné rady
- Štatistika BIG-IP ASM na paneli úloh BIG-IP
- Viditeľnosť aplikácií, vykazovanie a analytika
- Prevencia zberu webových údajov
- Skupinové incidenty s koreláciou porušení
- Integrácia pravidiel iRules a Fast Cache™
- Zachytenie reakcie pre platné alebo útočné požiadavky
- Akcelerátor SSL
- Brána firewall pre dátové centrum
- Sieťová a aplikačná brána firewall s certifikáciou ICSA
- Geolokačné blokovanie
- Správa kľúčov a zlyhaní (failover)
- Ukončenie relácie SSL a re-enkrypcia na webové servery
- Šifrovanie/dešifrovanie pre webové služby a overenie digitálneho podpisu
- Segmentácia siete VLAN
- Navrstvenie politiky na báze zraniteľnosti na existujúcu politiku BIG-IP ASM
- Podpora certifikátov na strane klienta
- Overovanie klientov cez protokol LDAP/RADIUS
- Vrstvenie modulov BIG-IP
- Lepšia ochrana pred hrozbami s externou službou IP Intelligence
- Podpora pre ICAP
- Integrácie rozšíreného hodnotenia zraniteľnosti s obmedzeným počtom voľných prehľadávaní
- Centralizovaný rozšírený reporting
- Zabezpečenie databáz s bránou Oracle
- Database Firewall
- Zabezpečenie aplikácií pre virtuálne prostredia
- Automatická synchronizácia politiky medzi viacerými zariadeniami
- Zabezpečenie aplikácií v privátnej službe typu cloud
- Podpora pre 64-bitové OS
- Podpora pre smerovacie domény
- Sprievodca nasadením - wizard pre zabezpečenie virtuálneho servera



ALEF DISTRIBUTION SK, s.r.o.
Galvaniho Business Centrum IV
Galvaniho 17/C
821 04 Bratislava 2
tel: +421 (2) 4920 3888
www.alef.com
sk-sales@alef.com

PRAGUE — BRATISLAVA — BUDAPEST