F5® BIG-IP® Advanced Firewall Manager™ (ďalej len „brána BIG-IP AFM“) je vysokovýkonná stavová sieťová brána firewall s architektúrou full proxy určená na ochranu dátových centier pred hrozbami, ktoré prenikajú do siete cez najčastejšie používané protokoly. Brána BIG-IP AFM je postavená na špičkovom radiči pre poskytovanie aplikácie (ďalej len „radič ADC“) od spoločnosti F5. Podnikom a poskytovateľom služieb prináša rozšíriteľnosť, flexibilitu, výkon a kontrolu, ktoré sú potrebné na obmedzenie tých najagresívnejších, masívne šírených distribuovaných útokov zahltením servera služby (ďalej len „útok DDoS“) ešte predtým, než sa im podarí preniknúť do dátového centra.

### Stavové zabezpečenie s architektúrou full proxy

Na rozdiel od tradičných brán firewall, brána BIG-IP AFM je postavená na architektúre full proxy operačného systému F5 TMOS. Prichádzajúce pripojenia klientov sú úplne ukončené, skontrolované z hľadiska rizika ohrozenia bezpečnosti, a až potom odovzdané serveru – za predpokladu, že nepredstavujú žiadnu hrozbu.
S architektúrou full proxy systému TMOS brána BIG-IP AFM získava podrobný prehľad o najčastejšie používaných vstupných protokoloch, ako sú HTTP, HTTPS, DNS, ICMP, či TCP a podporuje bohatú škálu služieb, ktoré rozširujú funkcie tradičnej stavovej brány firewall. S týmito funkciami brána získava detailnejší prehľad o pripojeniach a dokáže dáta spracovať a upraviť ešte predtým, než sú poslané napríklad na server.
V opačnom smere sa proxy používa aj na komunikáciu zo servera na klienta. Brána BIG-IP AFM dokáže z vrátených údajov vypustiť citlivé informácie, napríklad kódy odpovede protokolu, ktoré by mohli prezradiť informácie o sieti použiteľné na prieskumné útoky, a privátne údaje, ako sú čísla kreditných kariet, či sociálneho zabezpečenia.
Architektúra full proxy umožňuje ukončiť spojenie SSL, vynucovať politiky zabezpečenia a poskytovať iné služby súvisiace so zvyšovaním výkonu, ktoré organizáciám pomáhajú odstraňovať problémy súvisiace s volatilitou vo vnútri i mimo dátového centra.

## Centralizovaná správa politiky brány firewall

Veľké organizácie čelia rastúcemu problému s riadením konzistencie a účinnosti stavu zabezpečenia naprieč neustále rastúcim počtom zariadení s bránou firewall. Správcovia zabezpečenia sú príliš často nútení spravovať každé zariadenie samostatne, čím sa znižujú možnosti prevádzkovej škálovateľnosti a zvyšujú režijné náklady.
F5 BIG-IQ® je inteligentná platforma na správu a organizovanie zariadení F5 a služieb, ktoré tieto zariadenia poskytujú. Súčasť zabezpečenia BIG-IQ umožňuje centrálne spravovať brány firewall v prostredí s nasadením a správou niekoľkých zariadení BIG-IP AFM. Súčasť zabezpečenia BIG-IQ, nasadená buď ako zariadenie v dátovom centre, virtuálna edícia, či v prostredí SDDC zabezpečuje integrované sledovanie pravidiel brány BIG-IP AFM. Správcom umožňuje jednoducho spravovať politiky zabezpečenia naprieč rôznymi zariadeniami a rýchlo reagovať na meniace sa hrozby a neustále sa vyvíjajúce profily útokov.

Súčasť zabezpečenia BIG-IQ zjednodušuje správu životného cyklu politiky brány firewall pre všetky riešenia F5 na ochranu aplikácií a predstavuje centrálny bod pre riadenie a konsolidovaný náhľad na politiky zabezpečenia naprieč bránami BIG-IP AFM a zariadeniami so systémom BIG-IP® Application Security Manager™ (ASM).
Organizáciám súčasť zabezpečenia BIG-IQ prináša možnosti v oblasti vysokej škálovateľnosti a rozšírenia pri správe pravidiel brány firewall a konfigurovateľných prvkov v rámci celej infraštruktúry zabezpečenia BIG-IP – pre jednoduché vytváranie, úpravu, nasadenie a správu politík.

## Detailná viditeľnosť a hlásenia

Tímy pre IT a zabezpečenie vynakladajú úsilie na získavanie potrebných informácií o hrozbách a analýzu údajov, ktoré by im umožnili cielene zavádzať bezpečnostné opatrenia. Brána BIG-IP AFM organizáciám poskytuje detailný náhľad na útoky a techniky na ich obmedzenie, s ktorými dokážu prijímať informovanejšie rozhodnutia na zvýšenie celkovej účinnosti zabezpečenia.
S funkciami na vytváranie podrobných záznamov denníka a inteligentné hlásenie hrozieb brána BIG-IP AFM vytvára milióny záznamov v reálnom čase a poskytuje podrobný prehľad o útokoch DDoS pre hĺbkovú analýzu udalostí zabezpečenia. Správy vytvárané bránou BIG-IP AFM poskytujú jasné, výstižné a užitočné informácie o útokoch a trendoch vývoja. Informácie môžu byť zobrazené podľa úrovní, či rozdelené na strany. Správy obsahujú podrobné informácie o útokoch, priebehu hrozby a stave brány firewall.
S bránou BIG-IP AFM organizácie získavajú aj nástroj F5 Analytics, modul platformy BIG-IP, ktorý spája správy o útokoch DDoS z modulov BIG-IP ASM a BIG-IP AFM do jedného podrobného pohľadu všetkých hrozieb. F5 Analytics – pôvodne modul Application Visibility and Reporting, správcom umožňuje zobraziť a analyzovať

štatistické údaje získané o sieti a serveroch, i o samotných aplikáciách. Súčasťou brány BIG-IP AFM sú aj protokol SNMP a správy JSON na zjednodušenie posielania informácií o útokoch DDoS a iných dôležitých udalostiach do monitorovacích a forenzných systémov vyššej úrovne. Tieto systémy ponúkajú lepšie analytické funkcie, ktoré pomáhajú posilňovať celkový stav zabezpečenia organizácie.

## Zvýšená škálovateľnosť, výkon a spoľahlivosť

Brána BIG-IP AFM ponúka škálovateľnosť a výkon aj v prostrediach s tými najnáročnejšími požiadavkami na bránu firewall – s vynikajúcou rýchlosťou a priepustnosťou. Jediná platforma F5 podporuje až 576 miliónov súčasných pripojení, priepustnosť 640 Gb/s a 8 miliónov pripojení za sekundu na obmedzenie aj tých najväčších masívne šírených útokov. A v spojení s hardvérovou redundanciou, synchronizáciou, monitorovaním stavu a funkciami na automatické preklopenie a návrat služby po obnovení ponúka vyššiu garanciu dostupnosti a spoľahlivosti.

Riešenia spoločnosti F5 na ochranu aplikácií sú tvorené týmito modulmi BIG-IP:

- BIG-IP Advanced Firewall Manager (AFM) – táto rozšírená sieťová brána firewall je jadro brány firewall F5 pre poskytovanie aplikácií. Poskytuje úplnú viditeľnosť pre protokol SSL s možnosťou škálovania a pomáha obmedziť útoky DDoS na sieťovej vrstve i vrstve relácie.
- BIG-IP Local Traffic Manager (LTM) – ponúka služby rozšírenej správy sieťovej prevádzky, vyrovnávania zaťaženia a poskytovania aplikácií.
- BIG-IP Application Security Manager (ASM) – ponúka služby zabezpečenia aplikácií, prevencie zberu informácií z webových stránok a ochrany pred botmi, a obmedzenia útokov DDoS cez protokol HTTP.

## Funkcie a vlastnosti brány BIG-IP AFM

BIG-IP Advanced Firewall Manager je stavová brána firewall na architektúre full proxy pre rozšírenú ochranu siete.

### Brána firewall

| | |
|---|---|
| Detekcia anomálií na protokole | Áno – SYN, ICMP, ACK, UDP, TCP, IP**, DNS, ARP |
| Ochrana pred útokmi DoS a DDoS cez protokol L4 | Áno |
| Ochrana pred útokmi DoS a DDoS cez protokol SSL | Áno |
| Ochrana pre službu DNS a pred útokmi DDoS | Áno |
| Ochrana pred útokmi DoS a DDoS cez protokol HTTP | Áno |
| Spätné proxy cez protokol SSL | Áno |
| Reputácia* a geolokácia adries IP | Áno – vrátane identifikovania proxy Tor, malware a serverov typu C&C (príkazy a ovládanie) |
| Centrálna správa pomocou riadenia prístupu na základe rolí | Áno – so súčasťou zabezpečenia BIG-IQ |
| Správy protokolu SNMP | Áno |
| Analýza prítomnosti útoku DDoS na vzorke sieťovej prevádzky | Áno |
| * Licencia je predávaná samostatne.<br>** S podporou pre IPv4 a IPv6. | |
| | |

### IPsec

| | |
|---|---|
| Medzi lokalitami | Áno |
| Metódy vytvárania kľúčov | Ručné, výmena kľúčov v sieti internet (IKEv1 a IKEv2) |
| Metódy overovania | Zdieľaný kľúč, podpis RSA |
| Skupiny Diffie-Hellman | 1, 2, 5, 14, 15, 16, 17, 18 |
| Šifrovacie algoritmy | 3DES, AES-128, AES-192, AES-256, AES-GCM-128, AES-GCM-256 |
| Hashovacie a HMAC algoritmy | SHA-1, AES-GMAC-128, AES-GMAC-192, AES-GMAC-256 |

### Funkcie platformy

| | |
|---|---|
| Prenájom pre viac lokalít | Áno – so službou vCMP |
| Vysoká dostupnosť | Áno – aktívny–pasívny, alebo aktívny–aktívny |

SSL VPN

| | |
|---|---|
| Vzdialený prístup | Áno – s modulom BIG-IP APM |

| Škálovanie a výkon | VIPRION 4800 (8 ks B4300/B4340) | VIPRION 4480 (4 ks B4300/B4340) | VIPRION 2400 (4 ks B2150/B2250) | VIPRION 2200 (2 ks B2150/B2250) |
|---|---|---|---|---|
| Maximálna priepustnosť brány firewall | 640 Gb/s | 320 Gb/s | 160/320 Gb/s | 80/160 Gb/s |
| Počet pripojení za sekundu | 7,5 milióna | 4,8 milióna | 1,5 milióna/ 3,8 milióna | 750 000/ 1,9 milióna |
| Maximálny počet súčasných pripojení | 576 miliónov | 144 miliónov | 88 miliónov/ 176 miliónov | 44 miliónov/ 88 miliónov |

Podpora NAT, PAT, NAT Traversal.

Podpora IPv4 a IPv6.

## Výsledky laboratórneho testovania priepustností F5® BIG-IP® Advanced Firewall Manager™

Tieto testy merali výkon AFM a postupovali podľa metodológie testovania L3 firewallov.
Použité boli RFC:
- RFC2544 - UDP priepustnosti pri použití nasledujúcich veľkostí rámcov: 76, 256, 512, 1024, a 1518 bytes
- RFC6985 - UDP priepustnosť pri použití IMIX mixu celkosti rámcov. Pomer rámcov v IMIX nasleduje uvedený vzorec: AAAAAA BBBBB CCCC DDD EE F, kde jednotlivé písmena reprezentujú nasledovne:
A - 64 bytes
B - 76 bytes
C - 256 bytes
D - 512 bytes
E - 1024 bytes
F - 1518 bytes

Výkon pre RFC2544 pri použití B2250 bol nasledovný:
64b - 40Gbps
76b - 60Gbps
256b - 74Gbps
512b - 77Gbps
1024 - 78Gbps
1517 - 78Gbps

Výkon pre RFC6985 pri použití B2250 bol nasledovný:
IMIX - 70Gbps

## Dostupnosť brány BIG-IP AFM

Brána BIG-IP Advanced Firewall Manager je dodávaná spolu s ďalšími modulmi pre konkrétne podmienky použitia brány firewall na poskytovanie aplikácií, konkrétne:

| Názov balíka | BIG-IP AFM | BIG-IP LTM | BIG-IP ASM | BIG-IP APM | BIG-IP APM Lite (10 používateľov) |
|---|---|---|---|---|---|
| Application Delivery Firewall | ✓ | ✓ | | | ✓ |
| Application Delivery Firewall s Application Security (aplikačná bezpečnosť) | ✓ | ✓ | ✓ | | ✓ |
| Application Delivery Firewall s Access Management (menežment prístupov) | ✓ | ✓ | | ✓ | ✓ |
| Application Delivery Firewall a Application Security a Access Management (aplikačná bezpečnosť + menežment prístupov) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Advanced Firewall Manager Add-On (pre systémy s modulom BIG-IP LTM) | ✓ | | | | |

## Platformy VIPRION

Brána BIG-IP Advanced Firewall Manager je dostupná aj ako doplnkový modul pre systém BIG-IP Local Traffic Manager na modulárnej platforme F5 VIPRION®. Tento rám a architektúra kazetových serverov umožňujú jednoduché a postupné škálovanie podľa toho, ako rastie vaša sieť pre poskytovanie aplikácií. Podrobné informácie sa nachádzajú v Informačnom hárku platformy VIPRION.