KUPNÍ SMLOUVA

č. 286/OVZ/PV/2021

1. Kupující: **Univerzita Palackého v Olomouci**
veřejná vysoká škola zřízená zákonem č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů
Se sídlem: Křížkovského 511/8, 771 47 Olomouc
IČO: 61989592
DIČ: CZ61989592
Rektor: prof. MUDr. Martin Procházka, Ph.D.
Osoba oprávněná jednat ve věcech technických: [redacted]
Bankovní spojení: [redacted]
Číslo účtu:
(dále jen „Kupující") na straně jedné

a

2. Prodávající: **ALFA NOBEL s.r.o.**
Se sídlem: Denisova 277/16, 779 00 Olomouc
IČO: 04092121
DIČ: CZ04092121
Statutární orgán: Martin Svoboda, jednatel
Zapsán v obchodním rejstříku vedeném Krajským soudem v Ostravě, oddíl C, vložka 62321
Bankovní spojení: [redacted]
Číslo účtu:
Osoba oprávněná jednat ve věcech technických:
(dále jen „Prodávající") na straně druhé

uzavírají níže uvedeného dne, měsíce a roku podle ust. § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník"), tuto kupní smlouvu (dále jen „Smlouva") v rámci projektu *„Obnova a modernizace IT infrastruktury UP", reg. č. CZ.02.2.67/0.0/0.0/16_016/0002305 v rámci Operačního programu Výzkum, Vývoj a Vzdělávání.*

Kupující s Prodávajícím uzavírají tuto Smlouvu v důsledku skutečnosti, že Prodávající byl Kupujícím vybrán v otevřeném zadávacím řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v účinném znění, s názvem **„Zabezpečení webových informačních zdrojů pomocí aplikačních bran"** jako dodavatel této veřejné zakázky.

I. Předmět plnění

1. Předmětem této Smlouvy je dodávka rozšíření stávajícího elastického systému pro dodávání aplikací (ADS/ADC) podle specifikace, která tvoří nedílnou součást této Smlouvy jako její příloha č. 1 (dále jen „Zboží"). Prodávající není oprávněn odevzdat Kupujícímu větší množství Zboží ve smyslu § 2093 občanského zákoníku. Smluvní strany si ujednaly, že § 2099 odst. 2 občanského zákoníku se nepoužije.

2. Prodávající se zavazuje odevzdat za touto Smlouvou sjednaných podmínek Kupujícímu Zboží specifikované v příloze č. 1 této Smlouvy a umožnit mu nabýt vlastnické právo k tomuto Zboží, včetně provedení jeho instalace, konfigurace a migrace a provést zaškolení uživatelů Kupujícího kvalifikovaným pracovníkem a poskytovat záruční servis Zboží, za podmínek stanovených dále touto Smlouvou.

3. Kupující se zavazuje Zboží převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu sjednanými touto Smlouvou.

4. Součástí dodání předmětu Smlouvy je i doprava a dodání zákonných dokladů ke Zboží.

5. Prodávající ve smyslu § 2103 občanského zákoníku ujišťuje, že Zboží je bez vad.

6. Zboží musí být plně funkční, nové, nerepasované, bez dalších dodatečných nákladů ze strany Kupujícího.

II. Čas a místo dodání

1. Prodávající se zavazuje dodat a instalovat Zboží v místě dodání, včetně dodání všech zákonných dokladů ke Zboží, provedení všech zkoušek ověřujících splnění technických parametrů daných touto Smlouvou, provedení konfigurace, migrace a zaškolení uživatelů Kupujícího kvalifikovaným pracovníkem v rozsahu dle čl. V. odst. 2 této Smlouvy nejpozději do 60 kalendářních dnů od nabytí účinnosti této Smlouvy.

2. Místo dodání:
- Univerzita Palackého v Olomouci, Centrum výpočetní techniky, Biskupské náměstí 1, 779 00 Olomouc,
- Univerzita Palackého v Olomouci, Tř. Svobody 26, 779 00 Olomouc.

3. Smluvní strany si ujednaly, že ustanovení § 2126 a § 2127 občanského zákoníku o svépomocném prodeji se v případě prodlení Kupujícího s převzetím Zboží nepoužije.

4. Obalový materiál dodávaného Zboží musí být vyroben při využití lepenkových krabic nejméně z 50 % z recyklovaného materiálu; pokud se pro konečné balení používají plastové sáčky nebo fólie, musí být vyrobeny alespoň z 50 % z recyklovaného materiálu nebo musí být biologicky rozložitelné nebo kompostovatelné v souladu s definicemi uvedenými v normě EN 13432. Nesplnění povinnosti Prodávajícího dle tohoto ujednání Smlouvy se považuje za podstatné porušení Smlouvy s možností odstoupení Kupujícím od této Smlouvy. Odstoupení od této Smlouvy je v takovém případě účinné doručením písemného oznámení o odstoupení od Smlouvy druhé smluvní straně.

III. Kupní cena

1. Celková kupní cena Zboží činí **2.140.000,00 Kč bez DPH**. Prodávající je plátce DPH.

2. V kupní ceně jsou zahrnuty veškeré náklady spojené s dodáním Zboží a zisk Prodávajícího spojené s dodáním Zboží (zejména doprava Zboží na místo dodání, clo, pojištění, instalace Zboží, dodání všech zákonných dokladů ke Zboží, provedení konfigurace, migrace a zaškolení uživatelů Kupujícího kvalifikovaným pracovníkem, kompletní zajištění záručního servisu Zboží).

3. Kupní cena je sjednána jako cena pevná, nejvýše přípustná a maximální, zahrnuje veškeré náklady spojené s dodáním Zboží. Změna kupní ceny je možná pouze a jen za předpokladu, že dojde po uzavření této Smlouvy ke změnám sazeb daně z přidané hodnoty.

4. Prodávající odpovídá za to, že sazba daně z přidané hodnoty v okamžiku fakturace je stanovena v souladu s účinnými právními předpisy.

IV. Platební podmínky

1. Platba za dodávku Zboží proběhne na základě řádně vystaveného daňového dokladu (faktury), obsahujícího všechny náležitosti, ve lhůtě splatnosti do 30 kalendářních dnů ode dne jejího prokazatelného doručení Kupujícímu. Faktura bude vystavena Prodávajícím nejdříve po dodání Zboží, jeho řádné a úplné instalaci, dodání zákonných dokladů, provedení všech zkoušek ověřujících splnění technických parametrů daných touto Smlouvou, a provedení úvodního základního školení obsluhy v rozsahu dle čl. V. odst. 2 této Smlouvy, což bude potvrzeno písemným datovaným protokolem o dodání a instalaci Zboží. Dokladem o řádném splnění závazků uvedených v předchozí větě Prodávajícím je písemný datovaný předávací protokol opatřený podpisy oprávněných osob obou smluvních stran jednat ve věcech technických.

2. Prodávajícím vystavená faktura musí obsahovat všechny náležitosti daňového dokladu v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a náležitosti obchodní listiny dle § 435 občanského zákoníku a současně identifikaci Smlouvy, na jejímž základě bylo plněno. Fakturu Prodávající podpisem osoby oprávněné ji vystavit. Na vystavené faktuře bude vyznačen název a registrační číslo projektu a číslo této Smlouvy dle záhlaví Smlouvy.

3. Nebude-li faktura vystavená Prodávajícím obsahovat některou povinnou náležitost nebo Prodávající chybně vyúčtuje cenu nebo DPH, je Kupující oprávněn před uplynutím lhůty splatnosti vrátit fakturu Prodávajícími k provedení opravy s vyznačením důvodu vrácení. Prodávající provede opravu vystavením nové faktury. Dnem odeslání vadné faktury Prodávajícímu přestává běžet původní lhůta splatnosti a nová lhůta splatnosti běží znovu ode dne doručení nové faktury Kupujícím.

4. Smluvní strany se dohodly na tom, že závazek zaplatit kupní cenu je splněn dnem odepsání příslušné částky z účtu Kupujícího ve prospěch účtu Prodávajícího uvedeného v záhlaví této Smlouvy.

5. Prodávající zajistí řádné a včasné plnění finančních závazků svým poddodavatelům, kdy za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá Prodávajícímu k provedení závazků vyplývajících ze Smlouvy, a to vždy nejpozději do 15 kalendářních dnů od obdržení platby ze strany Kupujícího za konkrétní

plnění (pokud již splatnost poddodavatelem vystavené faktury nenastala dříve). Prodávající se zavazuje přenést totožnou povinnost do dalších úrovní dodavatelského řetězce a zavázat své poddodavatele k plnění a šíření této povinnosti též do nižších úrovní dodavatelského řetězce. Kupující je oprávněn požadovat předložení dokladů o provedených platbách poddodavatelům a smlouvy uzavřené mezi Prodávajícím a poddodavateli. Nesplnění povinností Prodávajícího dle tohoto ujednání Smlouvy se považuje za podstatné porušení Smlouvy s možností odstoupení Kupujícím od této Smlouvy. Odstoupení od této Smlouvy je v takovém případě účinné doručením písemného oznámení o odstoupení od Smlouvy druhé smluvní straně.

V. Instalace Zboží a zaškolení obsluhy

1. V rámci instalace Zboží v místě dodání, je Prodávající povinen prokázat zejména, nikoliv však výlučně, plnou funkčnost a splnění všech parametrů Zboží v souladu s nabídkou Prodávajícího, která tvoří nedílnou součást této Smlouvy (příloha č. 1 této Smlouvy).

2. Prodávající se zavazuje provést základní úvodní školení obsluhy dodávaného Zboží, které je podmínkou pro řádné předání a převzetí Zboží v rozsahu min. 1 x 2 hodiny pro min. 1 osobu ze strany Kupujícího. Odborně kvalifikovaní servisní technici, popř. aplikační specialisté provedou školení obsluhy, ve kterém bude zahrnuto:
   - o zapnutí/vypnutí zařízení,
   - o monitoring chyb,
   - o upgrade software,
   - o přepnutí dodávaného clusteru ADS na záložní prvek dodávaného řešení včetně přepnutí na stávající virtuální edici WAF Kupujícího.

3. Veškerá školení proběhnou v místě instalace zařízení, pokud nebude dohodnuto písemně jinak osobami oprávněnými jednat ve věcech technických za smluvní strany. Veškeré náklady spojené s výše uvedenými školeními (vč. pobytu servisního technika a aplikačního specialisty) hradí Prodávající.

4. Prodávající se zavazuje odvést a zlikvidovat veškerý odpad, zejm. obaly a zbytky materiálů použitých při plnění závazků z této Smlouvy, v souladu s příslušnými ustanoveními zákona č. 185/2001 Sb., o odpadech a o změně některých dalších zákonů, ve znění pozdějších předpisů, a dalšími příslušnými právními předpisy; doklady o likvidaci odpadů je Prodávající povinen na požádání Kupujícímu předložit.

VI. Odpovědnost Prodávajícího za vady a záruka za jakost

1. Prodávající poskytuje na Zboží záruku za jakost podle § 2113 a násl. občanského zákoníku v délce 24 měsíců ode dne podpisu předávacího protokolu dle čl. IV. odst. 1 této Smlouvy.

2. Nejpozději do 4 hodin od okamžiku ohlášení servisního požadavku Kupujícím (telefon, email, helpdesk) Prodávající v době záruky potvrdí přijetí tohoto servisního požadavku (telefon, email, helpdesk). Prodávající bude dále v době záruky garantovat reakce na servisní požadavek Kupujícího minimálně NBD (Next Business Day). Jednotlivé vady v záruční době musí být pak odstraněny nejpozději do 10 kalendářních dnů ode dne zahájení odstraňování vad (kdy dnem zahájení odstraňování vad se rozumí reakce na servisní požadavek Kupujícího), nedohodnou-li se osoby oprávněné jednat ve věcech technických za smluvní strany písemně jinak. Jednotné kontaktní místo pro nahlášení servisních požadavků

a oznamování vad: tel.: [redacted]

3. Prodávající se zavazuje k poskytování hot-line Prodávajícího a k provádění bezplatného plného servisu dodaného zboží, včetně aktualizací software, po celou dobu trvání záruční doby. Náklady na provádění záručního plného servisu dodaného zboží tvoří součást kupní ceny dle čl. V. odst. 1 této Smlouvy.

VII. Licenční ujednání

1. Veškeré licence budou dodány spolu se Zbožím dle této Smlouvy. Instalace software a cena licencí je zahrnuta v celkové kupní ceně. Prodávající je povinen zajistit, aby na Kupujícího v rámci poskytnutí licence přešla veškerá nezbytná oprávnění k užívání dodaného software Prodávajícího i třetích osob na dobu neurčitou, aby mohl být naplněn účel této Smlouvy. Prodávající prohlašuje, že je oprávněn poskytnout Kupujícímu licence k dodanému software podle této Smlouvy a že jak poskytnutím licence podle této Smlouvy, tak výkonem licenčních práv Kupujícím v souladu s touto Smlouvou nebudou porušena žádná práva, zejména pak autorská práva třetí osoby. V případě uplatnění práv k duševnímu vlastnictví třetí osobou je Prodávající povinen ihned Kupujícího o takovém nároku nebo řízení informovat.

2. Ukončením této Smlouvy z jakéhokoli důvodu, kterýmkoli způsobem a kteroukoli ze smluvních stran, vyjma odstoupení od Smlouvy s účinností od počátku, nebude dotčena žádná Kupujícímu poskytnutá licence, která zůstává i nadále Kupujícímu zachována v plném rozsahu.

3. V případě, že Prodávající poruší některé z výše uvedených licenčních ujednání či vyjde najevo, že prohlášení Prodávajícího jsou nepravdivá, jedná se o podstatné porušení povinností dle této Smlouvy. Prodávající je na základě výzvy Kupujícího povinen, bez dalších nákladů účtovaných Kupujícímu, podle druhu porušení

- napravit vzniklý stav, který je v rozporu s těmito licenčními ujednáními nebo s právními předpisy;
- zajistit licence v potřebném rozsahu pro naplnění účelu této Smlouvy;
- zajistit jinou nápravu tak, aby byl zajištěn účel této Smlouvy.

VIII. Utvrzení závazku

1. Smluvní strany si pro případ porušení smluvené povinnosti ujednávají smluvní pokuty v podobě, jak je upravují následující odstavce Smlouvy. Ani jedna ze smluvních stran ujednané smluvní pokuty nepovažuje za nepřiměřené s ohledem na hodnotu jednotlivých utvrzovaných smluvních povinností.

2. Prodávající se zavazuje uhradit Kupujícímu smluvní pokutu ve výši 0,2 % z celkové kupní ceny bez DPH za každý i započatý den prodlení se smluvně stanoveným termínem dodání ve smyslu čl. II. odst. 1 této Smlouvy.

3. Prodávající se zavazuje uhradit Kupujícímu smluvní pokutu ve výši 0,2 % z celkové kupní ceny bez DPH za každý i započatý den po marném uplynutí lhůty k nastoupení k opravě nebo lhůty k opravě Zboží v době záruky v souladu s čl. VI. této Smlouvy, a to za každý jednotlivý případ.

4. Smluvní strany se dohodly, že § 2050 občanského zákoníku se nepoužije, tj. že se smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně v plné výši vedle smluvní pokuty.

5. Splatnost vyúčtovaných smluvních pokut je 30 kalendářních dnů od data doručení písemného vyúčtování příslušné smluvní straně a za den zaplacení bude považován den odepsání částky smluvní pokuty z účtu příslušné smluvní strany ve prospěch účtu, který bude uveden ve vyúčtování smluvní pokuty.

6. Smluvní pokuty je Kupující oprávněn započíst ve smyslu ust. § 1982 a násl. občanského zákoníku proti i nesplatné pohledávce Prodávajícího na úhradu kupní ceny dle této Smlouvy.

IX. Závěrečná ujednání

1. Prodávající je osobou povinnou spolupůsobit při výkonu finanční kontroly ve smyslu ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, ve znění pozdějších předpisů. Tyto závazky Prodávajícího se vztahují i na jeho smluvní partnery, podílející se na plnění této Smlouvy.

2. Prodávající se zavazuje zajistit v rámci plnění této Smlouvy legální zaměstnávání osob a zajistí pracovníkům podílejícím se na plnění Smlouvy férové a důstojné pracovní podmínky. Férovými a důstojnými pracovními podmínkami se rozumí takové pracovní podmínky, které splňují alespoň minimální standardy stanovené pracovněprávními a mzdovými předpisy. Prodávající je povinen zajistit splnění požadavků tohoto ustanovení Smlouvy i u svých poddodavatelů. Nesplnění povinností Prodávajícího dle tohoto ujednání Smlouvy se považuje za podstatné porušení Smlouvy s možností odstoupení Kupujícím od této Smlouvy. Odstoupení od této Smlouvy je v takovém případě účinné doručením písemného oznámení o odstoupení od Smlouvy druhé smluvní straně.

3. Kupující si vyhrazuje právo zveřejnit obsah uzavřené Smlouvy.

4. Tato Smlouva se v otázkách v ní výslovně neupravených řídí občanským zákoníkem a právním řádem České republiky.

5. Ujednání této Smlouvy jsou vzájemně oddělitelná. Pokud jakákoli část závazku podle této Smlouvy je nebo se stane neplatnou či nevymahatelnou, nebude to mít vliv na platnost a vymahatelnost ostatních závazků podle této Smlouvy a smluvní strany se zavazují nahradit takovouto neplatnou nebo nevymahatelnou část závazku novou, platnou a vymahatelnou částí závazku, jejíž předmět bude nejlépe odpovídat předmětu původního závazku. Pokud by Smlouva neobsahovala nějaké ujednání, jehož stanovení by bylo jinak pro vymezení práv a povinností odůvodněné, smluvní strany učiní vše pro to, aby takové ujednání bylo do Smlouvy doplněno.

6. Změnit nebo doplnit tuto Smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této Smlouvy a podepsány oprávněnými osobami smluvních stran.

7. Kupující je oprávněn v souladu s ust. § 2001 občanského zákoníku odstoupit od této Smlouvy v případě:

7.1 prodlení Prodávajícího s dodáním Zboží delším než 10 kalendářních dnů,

7.2 nedodržení technické specifikace Zboží uvedené v nabídce Prodávajícího,

7.3 prodlení Prodávajícího se zahájením odstraňování vad o více než 10 kalendářních dnů.

Odstoupení od Smlouvy musí být učiněno písemně a nabývá účinnosti dnem doručení písemného oznámení druhé smluvní straně.

8. Prodávající není oprávněn bez souhlasu Kupujícího postoupit svá práva a povinnosti plynoucí z této Smlouvy třetí osobě.

9. Ohledně doručování zásilek týkajících se plnění této Smlouvy odesílaných Prodávajícím s využitím provozovatele poštovních služeb se § 573 občanského zákoníku nepoužije.

10. Prodávající bere na vědomí, že tato Smlouva včetně všech jejích příloh podléhá povinnému uveřejnění podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, v účinném znění.

11. Tato Smlouva nabývá platnosti dnem jejího podpisu posledním účastníkem této Smlouvy a účinnosti dnem uveřejnění této Smlouvy Kupujícím v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, v účinném znění.

12. Tato Smlouva je vyhotovena v elektronické podobě.

13. Prodávající bere na vědomí, že Kupující je povinen dodržet požadavky na publicitu v rámci programů strukturálních fondů stanovené v nařízení Evropského parlamentu a Rady (EU) č. 1303/2013 a pravidel pro publicitu v rámci OP VVV, a to ve všech relevantních dokumentech, týkajících se daného předmětu Smlouvy, ve všech dodatcích ke Smlouvě a dalších dokumentech vztahujících se k dané veřejné zakázce a v této souvislosti se zavazuje poskytnout Kupujícímu případně veškerou součinnost, kterou lze po něm spravedlivě požadovat.

14. Prodávající se zavazuje, že umožní všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je plnění dle této Smlouvy hrazeno, provést kontrolu dokladů souvisejících s tímto plněním, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, v platném znění a zákon č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění). Všechny výstupy smluvního vztahu, u kterých tak specifikuje Kupující, musí obsahovat prvky publicity a to v rozsahu dle záhlaví této Smlouvy, nepožaduje-li Kupující jinak. Logo EU včetně textů, logo Operační program Výzkum, vývoj a vzdělávání (dále jen „OP VVV“) dle požadavků Kupujícího. Kupující je povinen zajistit a případně poskytnout materiály obsahující správnou podobu jednotlivých log.

15. Prodávající je povinen uchovat veškerou dokumentaci související s plněním dle této Smlouvy v souladu s Pravidly minimálně do uplynutí 2 let od předložení účetní závěrky OP VVV podle čl. 140 nařízení Evropského parlamentu a Rady (EU) č. 1303/2013, tj. nejméně do 31. 12. 2033, pokud český právní systém nestanovuje lhůtu delší. Řídící orgán OP VVV, případně jím pověřené subjekty (případně i další kontrolní orgány podle platných právních předpisů) budou mít k těmto dokumentům na vyžádání přístup.

16. Nedílnou součást této Smlouvy tvoří přílohy:

Příloha č. 1 – Nabídka Prodávajícího ze dne 29. 11. 2021

V Olomouci, dne 06.01.2022

Za Kupujícího:

.....
prof. MUDr. Martin Procházka, Ph.D.
rektor Univerzity Palackého v Olomouci

V Olomouci, dne 21.12.2021

Za Prodávajícího:

.....
Martin Svoboda
jednatel společnosti

Kalkulace nabídkové ceny

Popis produktu

		AWAF addon	
F5	2 ks	F5-ADD-BIG-AWF-I5XXX	BIG-IP Advanced Web Application Firewall Module for i5X00
F5	2 ks	F5-SVC-BIG-STD-L1-3	Level 1-3 Standard Service for BIG-IP (5x10)
		APM addon	
F5	1ks	F5-ADD-BIG-APMI56XXB	BIG-IP Access Policy Manager Base Module for i5600
F5	1ks	F5-SVC-BIG-STD-L1-3	Level 1-3 Standard Service for BIG-IP (5x10)

Celková cena **2.140.000,- Kč bez DPH**

V nabídkové ceně jsou zahrnuty zvýšené náklady spojené s vývojem cen vstupních nákladů. Cena je nejvýše přípustná. Není-li uvedeno jinak, tak ceny jsou v Kč bez DPH. Nabídka splňuje všechny podmínky zadávací dokumentace. V nabídkové ceně jsou zahrnuty veškeré požadavky, služby, práce, školení, implementace, dokumentace, záruky, licence, drobný instalační materiál a další, dle zadávací dokumentace.

V Olomouci dne 29.11. 2021

S úctou a přáním pěkného dne, za společnost ALFA NOBEL s.r.o.

[redacted]

[redacted] Digitálně podepsal [redacted]
Datum: 2021.11.29 10:34:54 +01'00'

[redacted]

F5 Advanced WAF

DATA SHEET

What's Inside

Proactive Application Protection

Applications are critical to your business. Without the right protection, however, they can become an attack vector that may ultimately lead to a data breach. Consider this alarming statistic: Organizations have an average of 765 web applications and these applications are the initial target of data breaches 53% of the time.[1]

Protect your organization and its reputation by maintaining the confidentiality, availability, and performance of the applications that are critical to your business with F5® Web Application Firewall (WAF) solutions.

F5 WAF solutions are deployed in more data centers than any enterprise WAF on the market. The comprehensive suite of F5 WAF solutions includes managed rulesets for Amazon Web Services (AWS); cloud-based, self-service, and managed service in the F5 Silverline® cloud-based service delivery platform; application delivery controller (ADC) integration with F5 BIG-IP® Application Security Manager™ (ASM)[2]; and F5 Advanced Web Application Firewall™ (Advanced WAF).

Advanced WAF redefines application security to address the most prevalent threats organizations face today:

- Automated attacks and bots that overwhelm existing security solutions.
- Web attacks that steal credentials and gain unauthorized access across user accounts.
- Application layer attacks that evade static security based on reputation and manual signatures.
- New attack surfaces and threats due to the rapid adoption of APIs.

Advanced WAF is built on proven F5 technology and goes beyond reactive security such as static signatures and reputation to proactively detect and mitigate bots, secure credentials and sensitive data, and defend against application denial-of-service (DoS).

Advanced WAF delivers flexible and comprehensive protections wherever apps reside and without compromising performance. Advanced WAF is offered as an appliance, virtual edition, and as a managed service—providing automated WAF services that meet complex deployment and management requirements while protecting your apps with great precision. It is the most effective solution for guarding modern applications and data from existing and emerging threats while maintaining compliance with key regulatory mandates.

[1] 2018 Application Protection Report

[2] BIG-IP ASM continues to be offered through F5 Good/Better/Best licensing.

Key benefits

Protect web and mobile applications from malicious bots

F5 secures an organization's most valued assets, applications, and sensitive data from bots, automated attacks, web scrapers, and exploits. Advanced WAF extends bot protection to mobile applications through the F5 Anti-Bot Mobile SDK, providing rapid deployment of mobile bot protection through an easy-to-use web portal without requiring any changes to the application or mobile device. Applications fused with mobile bot protection are supported in vendor and third-party application stores.

Safeguard credentials and sensitive data from theft and abuse

Advanced WAF secures credentials and sensitive data from theft and abuse, preventing data breaches and mitigating automated attacks that leverage previously stolen credentials. F5 BIG-IP DataSafe™ application layer encryption in Advanced WAF masks sensitive fields directly within the user's web browser, rendering data stolen by bad actors through client-side attacks useless. Using BIG-IP DataSafe, customers can encrypt data at the field level transparently, without requiring any changes on clients or Web servers. Comprehensive brute force mitigation including credential stuffing protection defends against automated attacks that leverage previously stolen credentials.

Defend against sophisticated application denial-of-service (DoS)

Advanced WAF discovers and fingerprints new and unusual traffic patterns without human intervention, distinguishing and isolating potential malicious traffic from legitimate traffic. This automated mitigation capability is based on a continuous feedback loop of client behavior and server stress. If anomalous behavior is detected, Advanced WAF automatically builds a dynamic signature and begins mitigating the attack. The effectiveness of the mitigation is then monitored through the continuous feedback loop. False positives are reduced while accuracy and performance are improved through continuous mitigation tuning as the attack starts, evolves, or stops.

Mitigate sophisticated threat campaigns

Threat Campaigns provide targeted signatures to protect organizations from pervasive attacks that are often coordinated by organized crime and nation states. Based on F5 Labs research, Threat Campaigns provide critical intelligence to fingerprint and mitigate sophisticated attacks with nearly real-time updates. Metadata is used to determine both malicious requests and malicious intent, and the high accuracy of Threat Campaign signatures immediately blocks active threats with low false positives and no learning cycle.

Protect APIs

As web applications expand from connected to collaborative via the extensive use of Application Programming Interfaces (APIs), Advanced WAF ensures that API methods are enforced on URLs. It also secures applications against API attacks that commonly go undetected by traditional firewalls. With a unique defense mechanism that guards XML, JSON, and GTW APIs through rate limiting, behavioral analysis, and anti-automation, Advanced WAF automatically detects application program interface threats, enforces strict policy rules for each use case, and blocks attacks and special content types—closing the back door on application threats. With F5 Access Manager™, API protection is improved through comprehensive authentication and token enforcement.

Ensure application security and compliance

Gain comprehensive security against sophisticated layer 7 attacks, blocking threats that evade traditional WAFs and enabling compliance with key regulatory mandates.

Turn on protection immediately

Simplify security with pre-built policies, thousands of out-of-the-box signatures, and a streamlined approach to policy management that decreases operational expenses.

Patch vulnerabilities fast

Identify and resolve app vulnerabilities in minutes with leading dynamic application security testing (DAST) integration and automatic virtual patching.

Deploy flexibly

Deploy as an appliance, in virtual or cloud environments, and as a managed service supporting multi-tenant services while incorporating external intelligence that secures against known IP threats.

Defend with proven advanced protections

Defend with highly programmable technology that dynamically adapts policies, proactively stops bots and DoS attacks, and demonstrates 99.89% overall security effectiveness.

Magnify threat knowledge

Easily understand your security status with detailed forensic analysis, full visibility into HTTP and WebSocket traffic, and rich insight into all events and user types.

Ensure Comprehensive Threat Protection

The volume and sophistication of attacks makes keeping up-to-date on security threat types and protection measures a challenge for application administrators and security teams. With industry-leading capabilities and superior flexibility, F5 Advanced WAF delivers advanced, cost-effective security for the latest web and mobile applications.

Advanced WAF protects credentials from theft and abuse, and secures any parameter from client-side manipulation by validating login parameters and application flow to prevent forceful browsing and logical flaws. It also allows organizations to effectively guard against existing and emerging layer 7 application attacks—preventing costly data breaches, thwarting DoS attacks, and maintaining compliance. Advanced WAF is the first leading WAF that supports the transition from AJAX/HTTP to WebSockets for greater efficiencies and less overhead with bi-directional streaming data. Advanced WAF also provides visibility into WebSocket traffic—enabling companies to transition to protecting chat sessions and streaming information feeds (such as stock tickers) from data exposure, tampering, and theft. Users benefit from an extensive database of signatures, dynamic signature updates, DAST integration, and the flexibility of F5 iRules® scripting for customization and extensibility.

Organizations rely on Advanced WAF to protect the world's most visited web applications wherever they reside, with the highest level of security and without compromising performance. Advanced WAF enables organizations to detect and mitigate layer 7 threats including web scraping, web injection, brute force, CSRF, JSON web threats, DoS-heavy URLs, and zero-day attacks—providing early warnings, while mitigating threats per policy.

It automatically defends against multiple, simultaneous application-layer threats including stealthy, low-bandwidth DoS attacks. Advanced WAF also stops in-browser session hijacking and reports regular and repeated attacks from IPs.

Using automatic learning capabilities, dynamic profiling, unique anomaly detection methods, and risk-based policies, Advanced WAF can impose needed protections to prevent even the most sophisticated attacks from ever reaching servers. When combined with F5 BIG-IP Local Traffic Manager™ (LTM), Advanced WAF filters attacks and accelerates applications for an improved user experience.

Continuous expert security research

F5's security research team helps ensure continuous development of Advanced WAF signatures, policies, and capabilities. Researchers explore forums and third-party resources, investigate attacks, reverse engineer malware, and analyze vulnerabilities to determine effective detection and mitigation methods that guard against zero-day threats, DoS attacks, and other evasive or evolving threats. Advanced WAF offers enhanced protection from advancements in technology, regular signature updates, threat intelligence, and tightening of existing capabilities.

Defend with proactive bot protections

An always-on defense is required to successfully identify and protect against automated DoS attacks, web scraping, and brute force attacks before they occur. F5 delivers proactive bot defense capabilities that effectively provide controls to help prevent these attacks from ever taking place. Using advanced defense methods and reputation matching to identify non-human users (such as JavaScript and CAPTCHA challenges, geolocation enforcement, and other techniques), Advanced WAF slows requests to distinguish bots and then drops those requests before they reach a server. Advanced WAF thoroughly inspects user interaction, analyzes the health of the server, and discerns transaction anomalies to help detect bots that may bypass client/application challenges, established rate limits, and other standard detection methods. It also automatically mitigates layer 7 attacks that show an unusual change in request patterns. Unique from other solutions, Advanced WAF provides security experts with greater control of bot defense enforcements, allowing them to force additional action (such as high-speed logging on block or challenge actions, JavaScript challenges, URI overrides, customized HTML redirects, and more) before mitigations are applied. The Advanced WAF bot defense capabilities provide the most effective prevention methods, allowing you to identify suspicious automated activity, categorize bots detected, and mitigate attacks with the highest level of precision. The F5 Anti-Bot Mobile SDK, in conjunction with Advanced WAF, extends F5's comprehensive bot protection to mobile applications without any changes to application code.

Track malicious user attempts

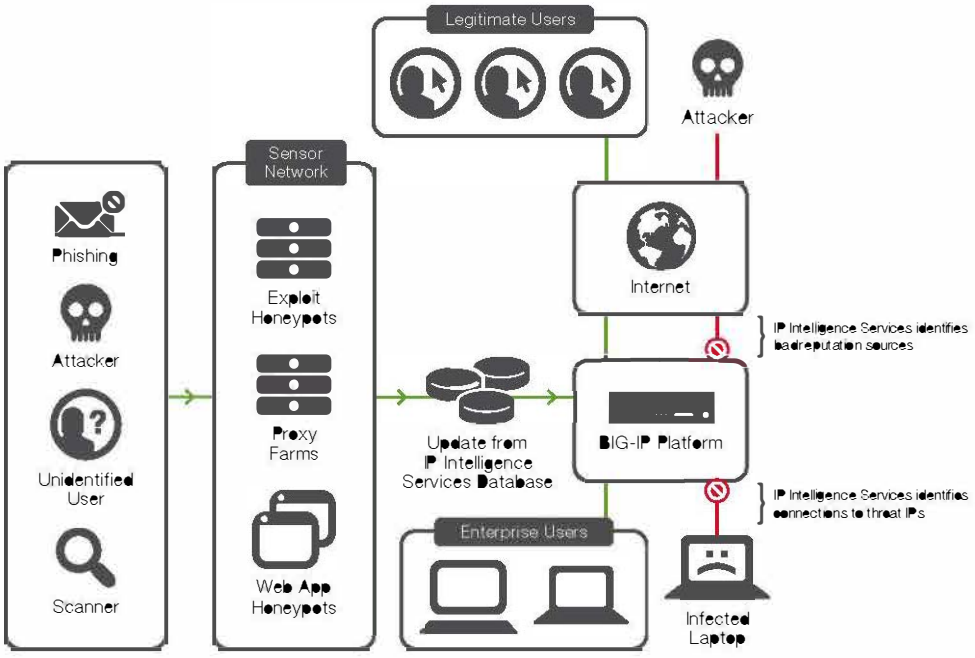
Distinguishing permitted users from bad actors whenever a website is visited helps minimize security risk and prevent malicious activity. With Advanced WAF, application security teams can employ device identification tracking techniques to identify specific end-users, application sessions, and attackers. This unique capability allows IT to easily distinguish human traffic from bot traffic, spot repeat visitors, prevent malicious attempts, and help WAFs more accurately mitigate brute force, session hijacking, web scraping, and DoS attacks.

Device identification tracking enables Advanced WAF to identify the same browser, even when users switch sessions or source IPs. When activated, Advanced WAF captures and saves unique device characteristics and attributes determines which clients are suspicious, and mitigates threats based on predefined settings. Whether an automated threat, DoS attack, headless browser, or human user, Advanced WAF can distinguish between repeat attackers and customer visitors for every WAF use case.

Block malicious IP addresses

Delivering today's rich and complex Internet content to users can expose an organization to a variety of potentially malicious attacks from rapidly changing IP addresses. Inbound and outbound botnet traffic, such as DoS and malware activity, can penetrate the organization's security layers. F5 IP Intelligence Services enhances automated security decisions with IP reputation intelligence. By identifying IP addresses and security categories associated with malicious activity, IP Intelligence Services can incorporate dynamic lists of threatening IP addresses from third parties into the F5 platform, adding context and automation to Advanced WAF blocking decisions. This adds granularity to Advanced WAF rules—allowing administrators to set an alarm, stop traffic, or fully block IPs based upon a specific IP reputation category while allowlisting approved IP addresses.

Additionally, Advanced WAF alleviates computational heavy mitigation of threats from known malicious IP addresses with a unique IP shun capability (accelerated denylisting). Instead of wasting cycles on traffic from badly behaving IPs, Advanced WAF immediately denylists IPs that repeatedly fail challenges or undergo high block ratios. This temporarily blocks malicious IPs in hardware at the network layer until IP intelligence feeds are up to date.



IP Intelligence Services gathers reputation data for use by F5 solutions.

Enabling secure encryption

As the increasing demand for data protection drives growth in encrypted traffic, it is important to transition to Perfect Forward Secrecy (PFS) while guarding against SSL/TLS attacks that threaten the security of applications and information in transit. Advanced WAF protects against malicious attempts to overcome SSL/TLS and compromise private keys, user passwords, and other sensitive information. It provides full SSL/TLS termination, and decrypts and re-encrypts terminated traffic—allowing complete inspection and mitigation of concealed, malicious threats. When Advanced WAF is combined with BIG-IP LTM, organizations also gain comprehensive SSL/TLS DDoS mitigation and SSL/TLS offload protection to secure against SSL/TLS attacks including SSL floods, POODLE, Heartbleed, and various memory-cracking tools.

Identify anomalous behavior

With Advanced WAF, IT can easily detect traffic that does not conform to normal behavior and evades usual volumetric protections—such as an uncommon increase or decrease in latency or the transactions rate. Advanced WAF can identify and uniquely block excessive failures to authenticate IP addresses generating a high volume of login attempts, as well as other anomalies in the typical traffic pattern. These include sessions opened at high rates or requesting too much traffic. Behavioral analytics and machine learning in Advanced WAF automatically monitor client and server traffic for anomalies in a continuous feedback loop.

Patch vulnerabilities immediately

Advanced WAF integrates with leading web application vulnerability scanners to allow you to easily manage assessments, discover vulnerabilities, and apply specific policies from a single location. These unique capabilities facilitate near-instantaneous mitigation of application assessment results, ensuring protection while developers correct vulnerable code—patching in minutes instead of weeks or months. With Advanced WAF, administrators can import testing results from DAST scanners, including scanners from WhiteHat, IBM, and QualysGuard, and layer a vulnerability-driven policy (received from F5 scanner integrations) on top of a current rapid deployment or SharePoint policy. When combined with WhiteHat Sentinel, Advanced WAF also detects and reports recent website changes to the scanner. This ensures scanning of otherwise overlooked URLs and parameters, and the application of specific policies—enabling organizations to secure their applications immediately after updating.

Advanced WAF DAST support helps IT deliver next-generation website security using simple, accurate, automated services. These services protect assets in a dynamic threat environment with more comprehensive assessments, zero false positives, and more manual and automated virtual patches than any other WAF solution.

Enforce geolocation-based blocking

Attacks are increasing from a variety of global sources. Advanced WAF enables you to block these attacks based on geolocation: states, countries, or regions. Administrators can easily select allowed or disallowed geolocations for strong policy enforcement and attack protection. Geolocation-based blocking also protects against anomalous traffic patterns from specific countries or regions, and enables traffic throttling based on location. Advanced WAF geolocation-based protection can be applied to a CAPTCHA challenge and to protect RAM cache and other resources from DDoS attacks.

Inspect SMTP and FTP

Advanced WAF enables SMTP and FTP security checks to protect against spam, viral attacks, directory harvesting, and fraud. Using default settings, administrators can easily configure security profiles to inspect FTP and SMTP traffic for network vulnerabilities and protocol compliance. Default settings can also be used to trigger alarms or block requests for violations.

SMTP security checks enable validation of incoming mail using several criteria, while disallowing or allowing common call methods used to attack mail servers. Additionally, administrators can set rate limits on the number of incoming messages, create allowlists and denylists, and validate DNS SPF records. FTP violations can be triggered for anonymous, passive, or active requests; specific FTP commands; command line length; and excessive login attempts. Administrators can use default SMTP/FTP settings for easy setup or customize profiles to address specific risks and more effectively ensure protocol compliance.

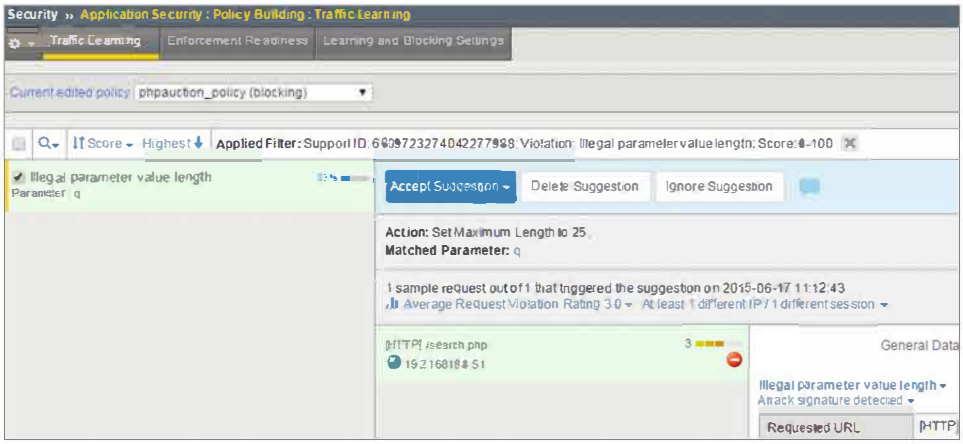
Streamline Learning, Deployment, and Management

Organizations want to turn on protections immediately without extensive security expertise. F5 Advanced WAF simplifies and automates configuration and policy deployment with pre-built security policies that provide out-of-the-box protection for common applications such as Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials, and Microsoft SharePoint. The validated policies also serve as a starting point for more advanced policy creation. This allows even novice users to rapidly deploy policies and immediately secure applications with little-to-zero configuration time needed.

Unified learning and dynamic policy building

At the heart of Advanced WAF is the unified learning and dynamic policy builder engine, which automates policy creation and tuning for increased operational efficiency and scalability. The policy builder engine automatically builds security policies around security violations, advanced statistics, and heuristics over time. It also understands expected behavior to affect more accurate traffic filtering.

By examining hundreds or thousands of requests and responses, the policy builder engine populates the security policy with legitimate elements more precisely than other WAFs. Dynamically generated policies are initially put into staging, then automatically moved from staging and enforced as they meet the rule thresholds for stabilization.
The policy builder engine supports automatic policy adaptation and learning following the occurrence of violations or as new parameters are observed. Policy maintenance is simplified by a GUI with a single-page view of all learning suggestions. One-click actions allow you to browse, search, accept, and ignore potential suggestions for policy adjustments, hardening policies with ease.



The enhanced learning GUI offers a single-page view of all learning suggestions.

Centralized management and monitoring

When you are deploying multiple Advanced WAF devices, F5 BIG-IQ® Centralized Management centralizes administration across your entire F5 infrastructure. Administrators get a consolidated view of all F5 devices, which helps to manage better relationships between devices, reduce IT overhead, and minimize configuration errors.

Advanced WAF provides an open API that supports easy integration to cloud/aaS virtual platforms and third-party policy management solutions. Engineers can fully configure and manage Advanced WAF policies from a programmatic interface that supports all policy management tasks, including login configuration, learning, semi-automatic tuning, utilization queries, and health monitoring. The Advanced WAF REST API exposes the entire range of Advanced WAF policy entities to support open models of WAF as a Service.

Leverage Rich, Actionable Reporting

F5 Advanced WAF provides powerful reporting capabilities that allow you to easily analyze incoming requests, track trends in violations through event correlation, generate security reports, evaluate possible attacks, and make informed security decisions. For security experts or generalists, Advanced WAF provides clear, discernable information with comprehensive visibility into attacks and changes in the threat landscape.

The Advanced WAF overview screen displays active security policies, security events and attacks, anomaly statistics, and networking and traffic statistics. Information can be saved or sent as an email attachment. Monitoring capabilities show how the application is being accessed and how it is behaving. The unique REST API supports easy integrations with higher-level SIEM or management services. Advanced WAF also offers predefined and customizable dashboards, charts, reports, and stats—highlighting DoS and brute force attacks, web scraping and IP enforcement, session tracking status, and more.

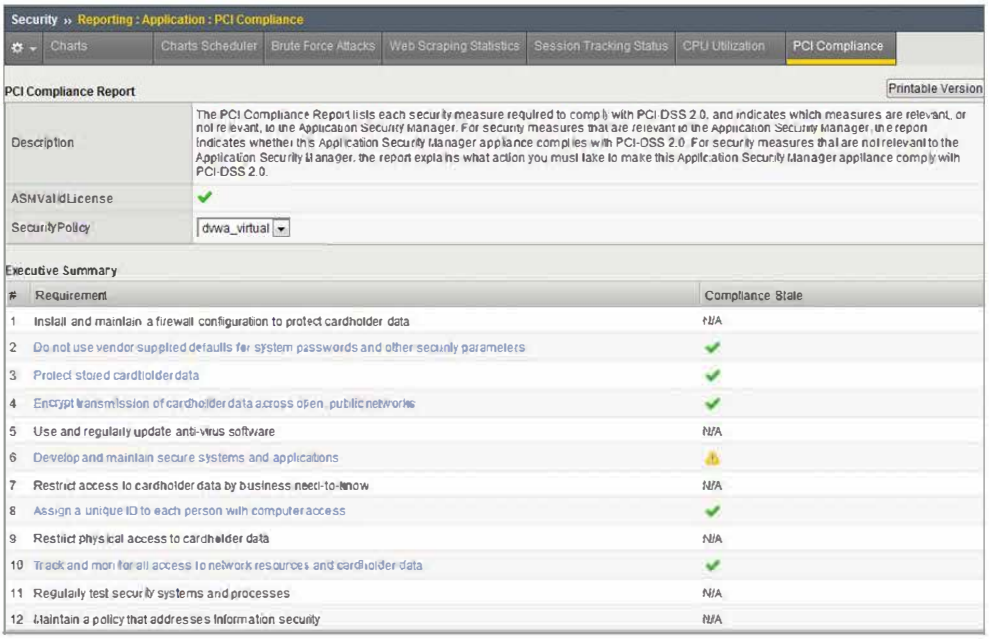
The security overview screen provides an easy view of what is happening on your system.

In-depth forensic analysis and database security

For deeper threat analysis, Advanced WAF integrates with high-speed indexing and search solutions like Splunk. These solutions offer deeper visibility into attack and traffic trends, long-term data aggregation, and identification of unanticipated threats before exposure occurs. Advanced WAF also supports database reporting for a real-time view into database activity and SQL statements generated by front-end users. Indexing and search solutions combine with Advanced WAF to provide richer forensic information for increased security effectiveness when mitigating threats.

Maintain compliance with industry and regulatory mandates

Advanced WAF makes it easy for organizations to understand and maintain regulatory compliance. Built-in security protection, logging and reporting, and remote auditing help organizations comply with industry security standards (including PCI DSS, HIPAA, BASEL II, FFIEC, SOX)—cost-effectively and without multiple appliances, application changes, or rewrites. With PCI reporting, Advanced WAF lists required security measures, determines if compliance is being met, and details necessary steps to becoming compliant.



Maintain compliance with industry and regulatory mandates.

Meet Complex Deployment Requirements

The explosion of the Internet of Things (IoT) has caused a tremendous impact on organizations. The number of web-facing applications that must be managed and secured has jumped dramatically. In addition, the increasing focus toward hybrid application deployment means that business apps now reside in multiple settings—data center, private cloud, and public cloud. As a result of these changes, new requirements are necessary for securing apps and transitioning WAF services from the data center to the cloud.

Hybrid WAF deployment models

F5 Advanced WAF offers flexible options that allow administrators to easily deploy firewall services close to the application. Administrators can also transition hardened security policies from data center appliances to Advanced WAF Virtual Edition (VE) in virtual and private cloud environments. Advanced WAF offers the same quality of protection and scalability with an appliance and software edition. Policies and iRules can seamlessly move between hardware devices and virtual appliances without manual updates.

F5's WAF technology supports application security in any environment, whether deployed on F5 hardware, as a virtual edition, or as a wholly managed cloud-based service.

F5 Silverline Web Application Firewall is built on F5 Advanced WAF, but is provided via the Silverline cloud-based application services platform and wholly deployed, set up, and managed by the highly specialized experts in the F5 Security Operations Center (SOC). With 24x7x365 expert support to protect web applications and data (and enable compliance with industry security standards), the Silverline Web Application Firewall service provides application protection without the need for capital investment and security expertise.

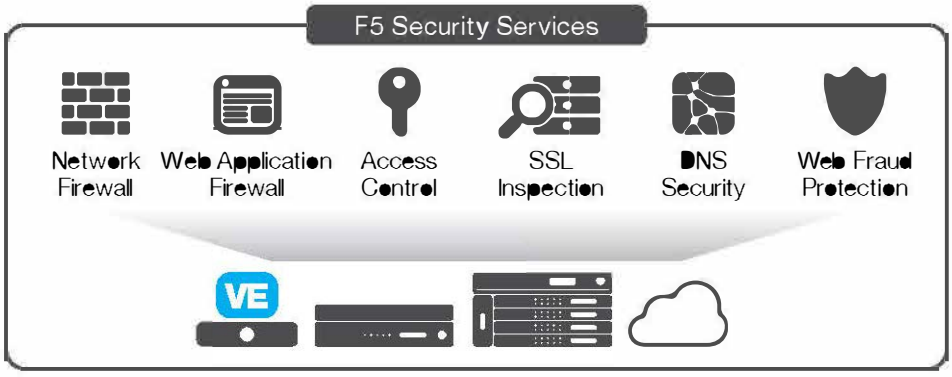
Running multiple instances of Advanced WAF

Advanced WAF uses F5 ScaleN® with F5 Virtual Clustered Multiprocessing™ (vCMP) to provide the most cost-effective application security implementation for managing large-scale deployments—whether you are a managed service provider offering WAFs as a service or simply managing a large number of Advanced WAF devices.

With Advanced WAF and vCMP-enabled systems, administrators can easily consolidate multiple firewalls onto a single device and allocate Advanced WAF resources in a more flexible and isolated manner for different customers, groups, applications, and services. vCMP enables you to run multiple instances of Advanced WAF on a single F5 platform with high-density firewall isolation through a combination of hardware and software. Guest firewalls can be clustered for easier administration and maintenance, and to ensure consistency throughout the firewall infrastructure. vCMP allows you to consolidate and better manage your security infrastructure, ensuring efficiencies and meeting service-level agreements (SLAs) with a dynamic, flexible WAF service infrastructure.

F5 Security Services

IT managers need a consolidated network and web application firewall solution to defend against multi-layered attacks, such as network and layer 7 events. F5 Advanced WAF, together with F5 Web Fraud Protection, F5 BIG-IP Advanced Firewall Manager™ (AFM), and F5 BIG-IP DNS, covers the threat spectrum—mitigating L3–L7 attacks, providing client-side fraud protection, and safeguarding the DNS infrastructure. When used with F5 Access Manager® (AM), Advanced WAF provides context-aware, policy-based access with simplified authentication, authorization, and accounting (AAA) management for web applications. As a component of F5's comprehensive security services, Advanced WAF benefits from other F5 modules to enable data center security, extensive application protection, and access management capabilities.



Advanced WAF, together with other BIG-IP modules, consolidates application protection and access management onto a single high-performing security platform.

F5 Advanced WAF Features and Specifications

Web Application Firewall

Deployment

Rapid deployment wizard with self-help hints	Yes
Unified learning and policy builder	Yes—with manual and automated policy building
Policy staging	Yes
Route domain support	Yes
VE, appliance, or managed service	Yes—managed services require Silverline License

WAF Security

Application layer encryption	Yes
Brute Force mitigation	Yes
Credential Stuffing protection	Yes
Behavioral denial-of-service (DoS) protection	Yes—protection for all applications
L7 DoS and DDoS detection including: HASH DoS, Slowloris, floods, Keep-Dead, XML bomb	Yes
Web scraping prevention	Yes
OWASP Top 10 prevention	Yes
Automated attack defense and bot detection	Yes
Advanced protections against threats including: Web injections, data leakage, session hijacking, HPP attacks, buffer overflows, shellshock	Yes
Mobile bot protection	Yes—with the F5 Anti-Bot Mobile SDK
Geolocation blocking	Yes
IP intelligence reputation services	Yes—with F5 IP Intelligence Services
SSL termination with re-encryption	Yes
Security incident and violation correlation	Yes
Client-side certification support	Yes
Client authentication	LDAP, RADIUS; more methods available with F5 Access Manager
Database security	Yes—with Oracle Database firewall
Response checking	Yes
Violation risk scoring	Yes
Web service encryption and decryption	Yes—and with signature validation
Device-ID detection and finger printing	Yes
Live signature updates	Yes
WebSocket traffic filtering	Yes
IP shunning (layer 3 denylisting in HW)	Requires F5 BIG-IP AFM license

Reporting and Analytics

Customizable charts and reports	Yes
Security overview report	Yes—drill down capabilities to granular details
Combined network and application attack report	Yes—with combined F5 BIG-IP AFM and F5 WAF deployment
WAF health monitoring	Yes
Compliance support PCI-DSS, HIPAA, SOX, Basel II	PCI-DSS, HIPAA, SOX, Basel II
Central management and reporting with role-based access control	Yes—requires F5 BIG-IQ Centralized Management
Automatic policy sync between WAF devices	Yes

Other

iRules and fast cache integration	Yes
SNMP reporting	Yes
REST API	Yes
ICAP support	Yes
DAST integration	Yes—WhiteHat, QualysGuard, and IBM
Fraud protection	Yes—requires F5 Fraud Protection Service license
SSL acceleration	Yes—core to the BIG-IP platform

BIG-IP Platform and TMOS support

Multi-tenancy	Yes—with F5 vCMP
High availability	Yes—active-passive or active-active
64-bit OS support	Yes
Application acceleration	Yes—requires F5 BIG-IP LTM
TCP optimization	Yes
Advanced rate shaping and QoS	Yes
F5 IPv6 Gateway™	Yes
IP port filtering	Yes
VLAN support	Yes
Secure SSL certificates from access	Yes
Integrates with BIG-IP AFM and F5 AM for complete data center security with identity and access management	Yes

F5 Advanced WAF

F5 Advanced WAF is available as a standalone solution or as an add-on module for BIG-IP Local Traffic Manager (LTM) on any F5 platform, and on BIG-IP LTM Virtual Edition (VE). F5 Access Manager (AM) is available as an add-on module to the Advanced WAF standalone appliance. F5 AM Lite (with 10 free user licenses) is included with any Advanced WAF standalone purchase. For detailed physical specifications, please refer to the BIG-IP System Hardware Data Sheet.

BIG-IP Platforms

Only F5's next-generation, cloud-ready application delivery controller (ADC) platform provides DevOps-like agility with the scale, security depth, and investment protection needed for both established and emerging apps. The new F5 BIG-IP iSeries appliances deliver quick and easy programmability, ecosystem-friendly orchestration, and record-breaking, software-defined hardware performance. As a result, customers can accelerate private clouds and secure critical data at scale while lowering TCO and future-proofing their application infrastructures. F5 solutions can be rapidly deployed via integrations with open source configuration management tools and orchestration systems.

In addition to iSeries, F5 offers the VIPRION® modular chassis and blade systems designed specifically for performance and for true on-demand linear scalability without business disruption. VIPRION systems leverage F5's ScaleN clustering technology so you can add blades without reconfiguring or rebooting.

Virtual editions of F5 software run on commodity servers and support the range of hypervisors and performance requirements. These virtual editions provide agility, mobility, and fast deployment of app services in software-defined data centers and cloud environments. See the F5 System Hardware, VIPRION, and Virtual Edition data sheets for more details. For information about specific module support for each platform, see the latest release notes on AskF5. For the full list of supported hypervisors, refer to the VE Supported Hypervisors Matrix.

F5 platforms can be managed via a single pane of glass with BIG-IQ Centralized Management.

BIG-IP iSeries Appliance

VIPRION Chassis

BIG-IP Virtual Editions

Virtual Editions

F5 Advanced WAF Virtual Edition (VE) can help you meet the needs of your virtualized environment by scaling to 20 cores/vCPUs.

F5 Advanced WAF VE

Hypervisors Supported:	• VMware vSphere Hypervisor 4.0, 4.1, 5.0, and 5.1 and vCloud Director 1.5 • Citrix XenServer 5.6 and 6.0 • Microsoft Hyper-V for Windows Server 2008 R2 and 2012 • KVM – Linux Kernel 2.6.32 (RHEL 6.2/6.3, CentOS 6.2/6.3)

Advanced WAF VE is also available as an Amazon Machine Image for use within Amazon Web Services.

amazon web services | Partner Network

F5 Global Services

F5 Global Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Global Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Global Services, contact consulting@f5.com or visit f5.com/support.

More Information

To learn more about F5 Advanced WAF, visit f5.com to find these and other resources.

Additional Resources

F5 Advanced WAF Overview

Advanced Application Threats Require an Advanced WAF

F5 Labs 2018 Application Protection Report

eBooks

Bots Mean Business

Credential Stuffing | A Security Epidemic

OWASP Top 10 and Beyond

Report

Gartner Web Application Firewall Magic Quadrant, 2018

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 [redacted] f5.com

Americas Asia-Pacific Europe/Middle-East/Africa Japan

[redacted]

BIG-IP Access Policy Manager

WHAT'S INSIDE

Simple, Secure, and Seamless Access to Any Application, Anywhere

Applications are gateways to your critical and sensitive data. Simple, secure access to your applications is paramount, but application access today is extremely complex. Apps can be hosted anywhere—in the public cloud, in a private cloud, on-premises, or in a data center. Ensuring users have secure, authenticated access anytime, anywhere, to only the applications they are authorized to access is now a significant challenge. There are different application access methods to deal with these complexities. There are also various sources for authorized user identity, as well as dealing with applications that require modern or more traditional authentication and authorization methods, single sign-on (SSO), federation, and more, in addition to ensuring a secure, simple user access experience to support and consider.

With digital transformation touching every part of an enterprise today, native cloud and Software as a Service (SaaS) applications are now the enterprise application standard. Many organizations, though, find they're unable or unwilling to migrate all their applications to the cloud. There may be mission-critical classic or custom applications that cannot or should not support migration to the public cloud or be easily replaced by a SaaS solution. Applications are being hosted in a variety of locations, with differing and many times disparate authentication and authorization methods that are unable to communicate with each other or work seamlessly across existing SSO or federated identity. They may be unable to support the newest identity methods, like Identity as a Service (IDaaS), and may not be equipped to support multi-factor authentication (MFA). And this doesn't even touch on the push toward a zero trust architecture.

F5® BIG-IP® Access Policy Manager® (APM) is a secure, flexible, high-performance access management proxy solution directing global access to your network, the cloud, applications, and application programming interfaces (APIs). Through a single management interface, BIG-IP APM consolidates remote, mobile, network, virtual, web, and API access. With BIG-IP APM, you can create, enforce, and centralize simple, dynamic, intelligent application access policies for all your apps, regardless of where or how they're hosted.

ICSA labs CERTIFIED SSL VPN FIREWALL-CORPORATE

KEY BENEFITS

Simplify access to all apps
Bridge secure access to on-premises and cloud apps with a single log in via SSO. It even works for applications unable to support modern authentication such as Security Assertion Markup Language (SAML), or OAuth and OpenID Connect (OIDC).

Zero trust application access
Identity Aware Proxy (IAP) delivers a zero trust operational model for application access based on identity awareness and granular context, securing every app access request without the need for a VPN.

Secure web access
Control access to web-based applications and web content centralizing authentication, authorization, and endpoint inspection via web app proxy.

Centralize and manage access control
Consolidate management of remote, mobile, network, virtual, web, and API access in a single control interface with adaptive identity federation, SSO, and MFA via dynamically enforced, context-based and identity-aware policies.

Streamline authentication and authorization
Adaptive identity federation, SSO, and MFA employing SAML, OAuth, and OIDC for a seamless and secure user experience across all apps.

BRIDGING SECURE ACCESS TO ALL APPLICATIONS

Modern authentication and authorization protocols—including Security Assertion Markup Language (SAML), and OAuth with OpenID Connect (OIDC)—reduce user dependency on passwords, increase security, and improve user experience and productivity. However, not all applications support modern authentication and authorization protocols. Many applications, such as classic applications or custom-built applications, support classic authentication and authorization methods, such as Kerberos, header-based, and more. This further complicates application access and security. The need to support different, disparate protocols unable to share user authentication and authorization information inhibits the use of SSO and MFA, which negatively affects user experience and application security. It also makes it difficult to adapt modern corporate password management and hygiene policies, and increases organizational costs as it becomes necessary to require and manage multiple access methods.

BIG-IP APM serves as a bridge between modern and classic authentication and authorization protocols and methods. For applications unable to support modern authentication and authorization protocols, like SAML and OAuth with OIDC, but which do support classic authentication methods, like Kerberos and header-based authentication, BIG-IP APM converts users' credentials to the appropriate authentication standard the application supports. BIG-IP APM ensures that users' organizations can use SSO to access any application anywhere—regardless of its location (on-premises, in a data center, in a private cloud, or in the public cloud as a native cloud or SaaS application), or whether or not it supports modern or classic authentication and authorization. This decreases the number of passwords users have to create, remember, and use, which helps stem the tide of credential-based attacks. BIG-IP APM enables compliance with modern corporate policies, like periodic password changes, that help combat stolen credentials. It also decreases the cost of having to purchase and maintain separate access solutions for applications that do not or cannot support modern authentication methods.

KEY BENEFITS (CONT.)

Defend your weakest links
Protect against data loss, malware, and rogue device access with comprehensive, continuous endpoint integrity and security checks.

Protect APIs
Enable secure authentication for REST and SOAP APIs and integrate OpenAPI or "Swagger" files to ensure appropriate authentication actions while saving time and cost.

Do it all at scale
Support all users easily, quickly, and cost-effectively with no performance trade-offs for security, even in the most demanding environments.

BIG-IP APM supports identity federation and SSO options by supporting connections initiated by both SAML identity providers (IdP) and service providers (SP) leveraging SAML 2.0. It empowers administrators to centrally enable and disable user authorized access to any identity-enabled applications, regardless of where they're hosted, saving time, and boosting administrative productivity.

Supporting the OAuth 2.0 open-standard for authorization enables BIG-IP APM to serve as a client, as an authorization delegate for SaaS applications, and to enhance the protection and authorization of APIs for web services.

INTELLIGENT INTEGRATION WITH IAM AND IDAAS

With support for SSO and Kerberos ticketing across multiple domains, BIG-IP APM enables additional types of authentication, such as U.S. Federal Government Common Access Cards (CAC) and IDaaS—such as Microsoft Azure Active Directory, Okta, and others—to access all applications regardless of location or support for modern authentication and authorization. For instance, users can be automatically signed on to back-end applications and services that are part of a Kerberos realm. This provides a seamless authentication flow once a user has been authenticated through a supported user-authentication mechanism. BIG-IP APM also supports smart cards with credential providers, so users can connect their devices to their network before signing in.

F5 partners with leading on-premises and cloud-based identity and access management (IAM) vendors, such as Microsoft, Okta, and Ping Identity. This integration enables local and remote user SSO via SAML, OAuth, or FIDO2 (U2F) to applications based on-premises or in a data center. For organizations that do not wish to replicate their user credential store in the cloud with IDaaS or cloud-based IAM offerings, working with its partners, F5 and BIG- IP APM work to help these organizations maintain control of on-premises user credentials. This is accomplished by creating a bridge between the IAM or IDaaS vendor's offering and the local authentication services. This bridge, or identity provider chain, leverages SAML to federate user identity.

SIMPLIFYING SECURE AUTHENTICATION

Through F5's extensive partner ecosystem, BIG-IP APM also integrates with most leading MFA solutions, including those from Duo (Cisco), Okta, Microsoft Azure Active Directory, and others. By integrating with your existing MFA solution, BIG-IP APM enables adaptive authentication, allowing various forms of single-, two-, or multi-factor authentication to be employed based on user identity, context, and application access. If needed, BIG-IP APM can also provide one-time password (OTP) authentication via email or SMS.

After the user has logged into an application, an additional means of authentication may be required to ensure secure access to mission-critical or particularly sensitive applications and files. This is commonly referred to as step-up authentication. BIG-IP APM supports step-up authentication for single- and multi-factor authentication. Any session variable may be used to trigger step-up authentication, and you can use additional authentication capabilities or select from our partner offerings. In addition, any session variable may be part of access policy branching (such as URL branching) per request policy. Step-up authentication policies may be based on applications, secure portions of applications, sensitive web URIs, extending sessions, or any session variable.

Many authentication solutions use application coding, separate web server agents, or specialized proxies that present significant management, cost, and scalability issues. With AAA control, BIG-IP APM enables you to apply customized access policies across many applications and gain centralized visibility of your authorization environment. You can consolidate your AAA infrastructure, eliminate redundant tiers, and simplify management to reduce capital and operating expenses.

As organizations focus on reducing user friction and increasing agility, their need to provide seamless access to all applications becomes a priority. BIG-IP APM enables organizations to reduce friction for users to remote access (SSL VPN). It also reduces friction for web applications. BIG-IP APM supports SSO across both remote access and web applications with a single login for either Apple Macs or Microsoft Windows devices (via Windows Hello for Business). Organizations can support the user login via U2F tokens (such as Yubico keys) or password-less FIDO2 via the F5 Edge Client to reduce user friction and increase application access security.

ZERO TRUST APPLICATION ACCESS

Many organizations—and maybe yours—are rapidly moving toward a zero trust security architecture. The pillars of a zero trust architecture are identity and context.

A zero trust approach to security means adopting a mindset that attackers have already infiltrated your network and are lurking, waiting for an opportunity or trigger to launch their attack. It eliminates the idea of a trusted insider within a defined network perimeter, assuming, at best, a limited secure network perimeter. It means never trusting users, even if they've already been authenticated, authorized, and granted access to applications and resources. A zero trust approach applies least privilege rights to user access, allowing users access rights only to the applications and resources they need to complete their tasks, and no more.

Identity and context awareness are also what define Identity Aware Proxy (IAP). IAP enables secure access to specific applications by leveraging a fine-grained approach to user authentication and authorization. IAP enables only per-request application access, which is very different than the broad network access approach of VPNs that apply session-based access, which is not a zero trust approach. With this approach, a VPN becomes optional to access applications. IAP enables organizations to create and enforce granular application access policies based on contextual attributes, for example, user identity, device integrity, and user location. IAP relies on application-level access controls, not network-layer rules. Configured policies reflect user and application intent and context. IAP requires a strong root of trusted identity to verify users and to stringently enforce what they're authorized to access.

Identity Aware Proxy is foundational to both a zero trust architecture and to F5 BIG-IP APM. BIG-IP APM and F5 Access Guard, a browser extension that coordinates with BIG-IP APM, deliver Identity Aware Proxy using a zero trust validation model on every application access request. Providing authenticated and authorized users secure access to specific applications, it leverages F5's best-in-class access proxy. BIG-IP APM centralizes user identity and authorization. Access is based on the principles of least privilege.

Through IAP, BIG-IP APM examines, terminates, or authorizes application access requests. Policies within BIG-IP APM can be created to:

- Verify user identity
- Check device type and posture
- Validate user authorization
- Confirm application integrity and sensitivity
- Confirm time and date accessibility

- Limit or halt access if the user's location or device posture is deemed incorrect, inappropriate, or insecure
- Request additional forms of authentication—including multi-factor authentication (MFA)— if the user's location or the sensitive nature of the applications or its data warrant it
- And more

Data from user and entity behavior analytics (UEBA) and other API-driven risk engines can be integrated seamlessly via BIG-IP APM's HTTP Connector, adding another level of security and application access control.

BIG-IP APM checks user device security posture via F5 Access Guard. However, BIG-IP APM and F5 Access Guard go beyond simply checking device integrity at authentication, delivering continuous, ongoing device posture checks to ensure user devices not only meet but adhere to endpoint security policies throughout the application access session. If BIG-IP APM detects any change in device integrity, it can either limit or stop application access, halting potential attacks before they can even be launched.

BIG-IP APM enforces access authentication using access control lists (ACLs) and authorizes users with dynamically applied layer 4 and layer 7 ACLs per session. Both L4 and L7 ACLs are supported based on the posture of users' devices as a policy enforcement point (PEP). Individual and group access to approved applications and networks is allowed by BIG-IP APM using dynamic, per-session L7 (HTTP) ACLs.

A guided configuration workflow allows organizations to host web applications protected by Identity Aware Proxy on a webtop, giving users a single catalog of all applications to which they're authorized. It offers a seamless user experience, as users can access all their applications from a single user interface, regardless of where the application is hosted. It also simplifies an administrator's workflow, enabling them to easily pick, choose, and modify the applications made accessible to specific user groups.

BIG-IP APM, through IAP, also simplifies application access for remote or home-based workers, better enables and secures application accessibility, and optionally eliminates the need for VPNs.

ROBUST ENDPOINT SECURITY

BIG-IP APM inspects and assesses users' endpoint devices before authentication and throughout a user's application access session with F5 Access Guard. A browser extension that provides device integrity data to BIG-IP APM, F5 Access Guard examines device security posture and determines if the device is part of the corporate domain. Based on the results, BIG-IP APM will apply dynamic ACLs to deploy context-based security. BIG-IP APM and F5

Access Guard include preconfigured, integrated endpoint inspection checks, including checks for OS type, antivirus software, firewall, file, process, registry value validation and comparison (Windows only), as well as device MAC address, CPU ID, and HDD ID. For mobile devices running iOS or Android, BIG-IP APM's endpoint inspection checks the mobile device UDID and jailbroken or rooted status.

RISK-BASED ACCESS USING THIRD-PARTY RISK ENGINES (HTTP CONNECTOR)

Many organizations have deployed third-party user and entity behavior analytics (UEBA) or risk engines. The ability to leverage an existing UEBA or risk engine to infuse real-time analytics and risk data within access control policies can help organizations ensure that access to networks, clouds, applications, and even APIs are regulated based on a risk profile. It's also important to address risk-based access to networks, clouds, apps, and APIs that's triggered by a variety of relevant variables.

Through HTTP Connector, BIG-IP APM integrates seamlessly with third-party UEBA and risk engines, leveraging their risk assessment via REST APIs as part of its policy-based access controls. This enables risk-based access to networks, clouds, apps, and APIs, further enhancing BIG-IP APM's Zero Trust IAP solution. BIG-IP APM's HTTP Connector leverages user group, domain, and network-based triggers to increase the enforceability of risk-based access. Risk-based access enhances security, providing greater visibility and analytics to determine whether to grant or deny access to your networks, cloud, applications, and APIs.

INTEGRATING WITH AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS

F5 BIG-IP APM and Microsoft Azure Active Directory (AD), when deployed together, enable seamless, secure access to all applications, regardless of where they're hosted or the type of authentication—modern or traditional—they use. BIG-IP APM and Microsoft Azure Active Directory have also extended application access security by integrating Microsoft Azure AD Conditional Access and BIG-IP APM. Microsoft Azure AD Conditional Access is a tool used by Azure AD to bring signals together in order to create and make access decisions and enforce organizational policies. Policies at their simplest are "if-then" statements: If a user wants to access a resource, then they must complete an action. By leveraging Azure AD Conditional Access policies in conjunction with BIG-IP APM, organizations can apply the right access controls when needed during users' application access sessions to keep their organization

and applications secure. Working together, Azure AD Conditional Access serves as the policy engine delivering real-time evaluation with BIG-IP APM serving as the enforcement point. BIG-IP APM and Azure AD Conditional Access unite to deliver continuous integrity and validation, and robustly enforce dynamic access control.

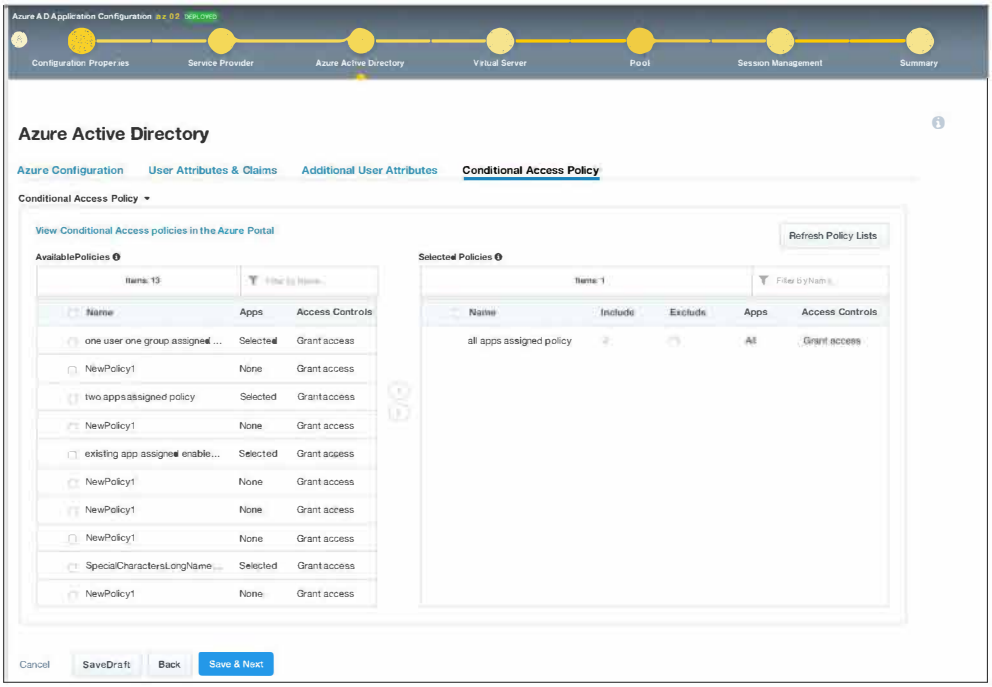


Figure 1: F5 BIG-IP APM seamlessly integrates Microsoft Azure Active Directory's Conditional Access to deliver an even more granular layer of access security to better secure zero trust environments.

PROTECTING APIS

APIs are the connective tissue in modern application architectures. Attackers are leveraging APIs to launch attacks because they're ripe for exploitation: Many organizations expose APIs to the public and their supply chain partners or they inadvertently leave them unprotected.

While attackers are exploiting APIs to launch attacks, organizations can ensure API security through strong authentication, especially if it's adaptable and protected by consistent, flexible authentication and authorization policies. BIG-IP APM enables secure authentication for REST or SOAP APIs. It also ensures appropriate authorization actions are taken. BIG-IP APM supports and imports OpenAPI 3.0 (Swagger) files, saving time and cost when developing API protection policies, while ensuring accurate API protection policies are in place. Quotas, allow-lists, and deny-lists can be configured for rate limiting API requests.

SECURING CREDENTIALS

User credentials are like the keys to the kingdom: All an attacker needs to do is steal one set of user credentials and they can enjoy unfettered access to your organization's network, clouds, and apps.

BIG-IP APM's credential protection, as part of an optional license of BIG-IP DataSafe™, secures credentials from theft and reuse. It protects against Man-in-the-Browser (MitB) attacks with real-time, adaptable login encryption, and encrypts user credentials entered into its webtop login. BIG-IP APM, in conjunction with BIG-IP DataSafe, renders the credentials unreadable and unusable, even in the unlikely event an attacker successfully steals them. BIG-IP APM also ensures login security for all applications associated via federation.

BIG-IP APM also supports server authentication via Client Certificate Constrained Delegation (C3D). By employing C3D, BIG-IP APM addresses certificate-based authentication, limiting the need for and use of credentials. With C3D, organizations can implement stronger encryption protocols and the latest key exchanges, as well as employ client certificate authentication, enable end-to-end encryption in reverse proxy environments, leverage Perfect Forward Secrecy (PFS), and validate client certificates using Online Certificate Status Protocol (OCSP).

UNIFYING ACCESS FROM ANY DEVICE

BIG-IP APM is positioned between your applications and your users, creating a strategic application access control point. APM protects your public-facing applications by providing granular policy for identity- and context-aware user access, while consolidating your access infrastructure. It secures remote and mobile access to applications, networks, and clouds via SSL VPN or zero trust application access via Identity Aware Proxy. BIG-IP APM converges and consolidates all access—network, cloud, application, and API—within a single management interface. It also enables and simplifies the creation of easy-to-manage dynamic access policies.

BIG-IP APM creates a dynamic web-based application portal or webtop. The BIG-IP APM webtop shows and enables access only to the applications authorized for and available to a user based on their identity and context—regardless of where the applications are hosted—on-premises, in a data center, in a private cloud, in a public cloud, or offered as a service. This dynamic, user-specific application portal or webtop simplifies application access and enhances the user experience.

F5 BIG-APM enables secure access to applications, networks, and clouds via the BIG-IP Edge Client and F5 Access. The BIG-IP Edge Client is available for Apple macOS, Microsoft Windows, Linux platforms, and Chromebooks. F5 Access is an optional mobile client for ensuring secure access from mobile devices supporting Apple iOS and Google Android, and is available for download from the Apple App Store or Google Play.

BIG-IP Edge Client and F5 Access integrate with leading mobile device management (MDM) and enterprise mobility management (EMM) solutions—including VMware Workspace ONE (AirWatch), Microsoft Intune, and IBM MaaS360—to perform device security and integrity checks and to deliver per-app VPN access without user intervention. Context-aware policies are assigned based on a device's security state as determined by the MDM or EMM solution. These policies enable, modify, or disable application, network, and cloud access from the device. Hardware attributes may be mapped to a user's role to enable additional access control decision points. A browser cache cleaner automatically removes any sensitive data at the end of a user's session.

BIG-IP APM enables Datagram Transport Layer Security (DTLS) mode, supporting DTLS 2.0 for remote connections that secure and tunnel delay-sensitive applications. It supports IPsec encryption for traffic between branch offices or data centers. Per-app VPN via an application tunnel through BIG-IP APM enables access to a specific application without the security risk of opening a full network access tunnel.

The dynamic split tunneling capability in BIG-IP Edge Client provides a simple way for administrators to dynamically exclude Zoom, Microsoft 365, or Webex traffic in APM network access tunnels. Real-time, latency-sensitive traffic won't be slowed down by going through a tunnel and being encrypted, which could affect user experience. This also enables administrators to easily manage which traffic they want to go through tunnels and how that traffic should be handled.

STREAMLINE VIRTUAL APPLICATION ACCESS

Virtual desktop and application deployments must scale to meet the needs of thousands of users and hundreds of connections per second. BIG-IP APM serves as a gateway for virtual application environments. It includes native support for Microsoft Remote Desktop Protocol (RDP), allowing Microsoft RDP to be available on non-Windows platforms, including macOS, Linux, Apple iOS, and Google Android. It also enables Microsoft RDP to work with any Microsoft, Apple, or Google web browser, or RDP app installed. BIG-IP APM also supports Citrix Virtual Apps and Desktops, and Citrix StoreFront, consolidating support for Citrix desktop and application virtualization infrastructure. It also delivers security proxy access for VMware Horizon. Administrators can control the delivery and security components of enterprise virtualization solutions via BIG-IP APM's unified access, security, and policy management. These scalable, high-performance capabilities simplify user access and control in hosted virtual desktop environments. BIG-IP APM delivers simple, broad virtual application and desktop support.

VISUAL POLICY EDITOR (VPE)

Through its advanced graphical Visual Policy Editor (VPE), BIG-IP APM makes designing and managing granular access control policies on an individual or group basis fast and simple. With VPE, you can efficiently create and edit dynamic access policies in just a few clicks. BIG-IP APM's VPE can define rules per URL path. By centralizing and simplifying the management of contextual policies, you can efficiently direct fine-grained user access to applications, networks, and clouds.

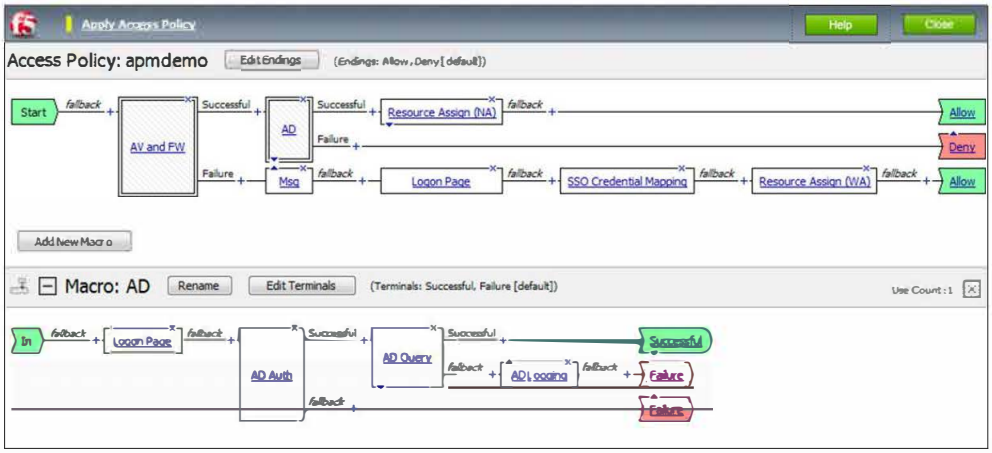


Figure 2: The BIG-IP APM advanced VPE makes it fast and easy to create, modify, and manage granular identity- and context-based access policies.

BIG-IP APM lets you design access policies for authentication and authorization, as well as endpoint security checks, enforcing user compliance with corporate policies and industry regulations. One access profile may be defined for all connections coming from any device, or you can create multiple access profiles for different access methods from various devices. The VPE in BIG-IP APM can be used to create, modify, and manage ACLs quickly and easily.

ACCESS GUIDED CONFIGURATION (AGC)

BIG-IP APM includes an Access Guided Configuration (AGC) capability that simplifies the deployment and management of application access. The AGC guides administrators through a step-by-step process of setting up and deploying BIG-IP APM, saving your organization deployment time and cost. BIG-IP APM's AGC also empowers administrators to quickly and simply onboard and operationally manage the integration of classic mission-critical applications, such as SAP ERP, Oracle PeopleSoft, Oracle E-Business Suite (EBS), and

Oracle JD Edwards with Microsoft Azure AD. BIG-IP APM's AGC eliminates numerous steps previously required to bridge the access gap between applications that support modern authentication and apps that support classic authentication methods—greatly reducing the administrative overhead involved in modernizing those applications.

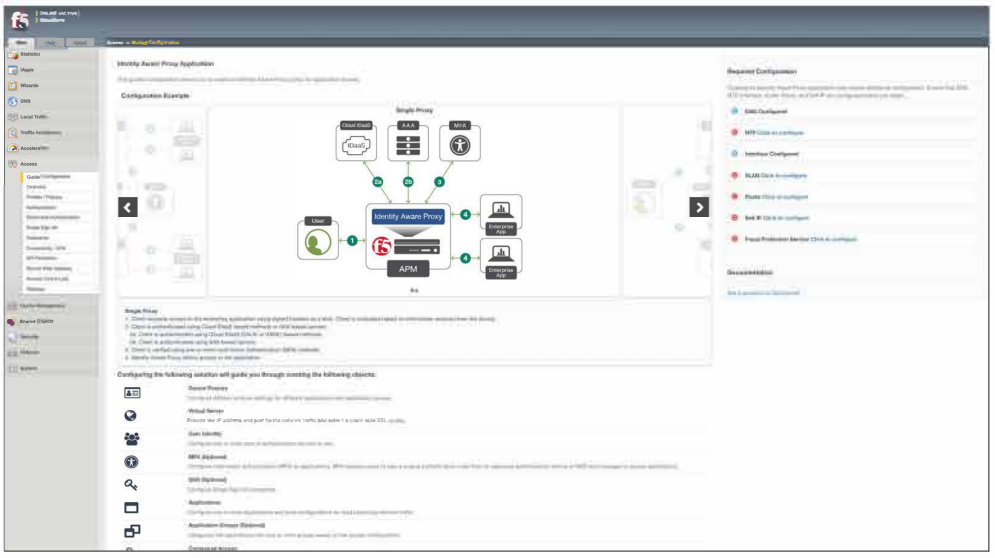


Figure 3: BIG-IP APM's Access Guided Configuration saves deployment time and cost.

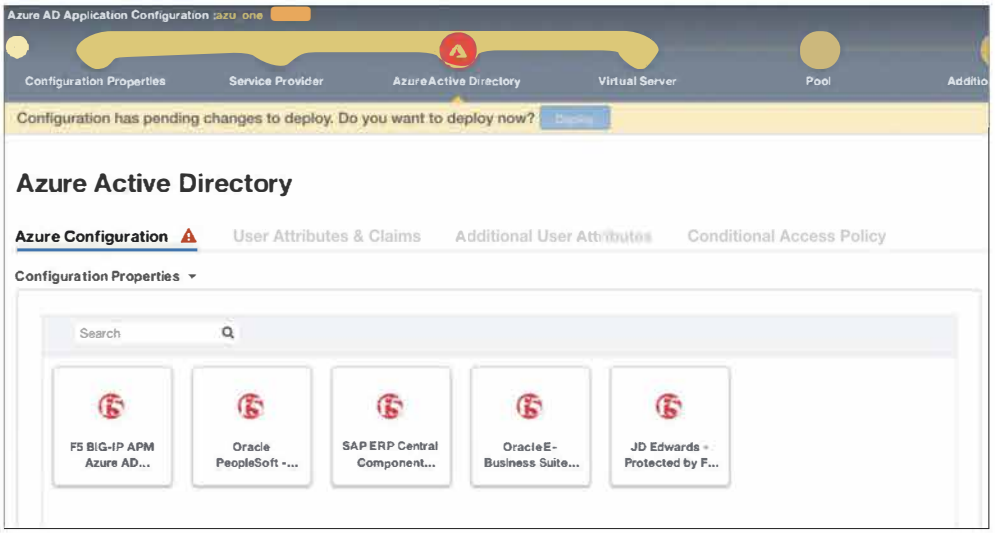


Figure 4: F5 BIG-IP APM's Access Guided Configuration enables quick, simple onboarding and management of custom applications and classic applications, such as SAP ERP, Oracle PeopleSoft, Oracle E-Business Suite (EBS), and Oracle JD Edwards with Microsoft Azure AD.

CENTRALIZE ACCESS POLICY MANAGEMENT

For organizations with multiple deployments of BIG-IP APM, F5 BIG-IQ® Centralized Management will efficiently manage them. It manages policies for up to 100 BIG-IP APM instances, enabling you to import, compare, edit, and update granular access policies across multiple user devices. With BIG-IQ Centralized Management and BIG-IP APM, you can import configurations from a master "source" BIG-IP APM instance, simplifying access policy distribution. You may also edit device- or location-specific objects directly on BIG-IQ Centralized Management and propagate them throughout your BIG-IP APM deployment. You can easily view the differences between current and proposed access configurations.

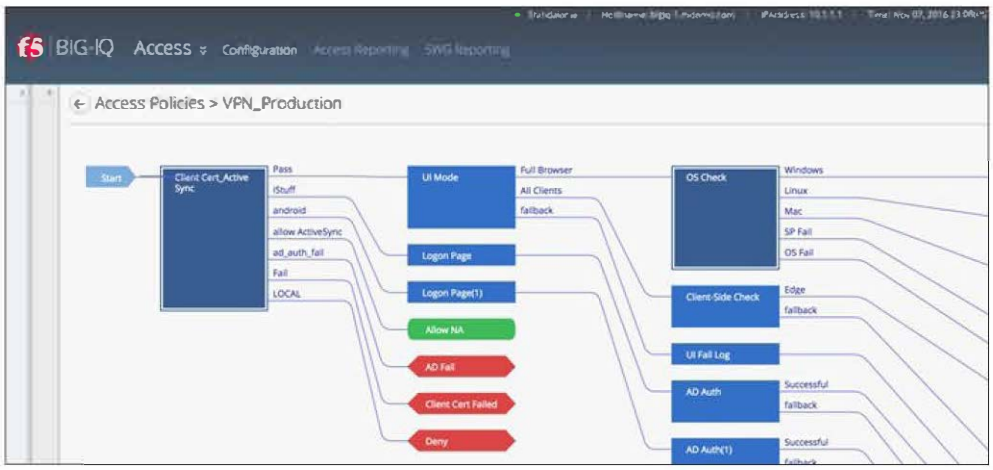


Figure 5: BIG-IQ Centralized Management enables the import, comparison, editing, and updating of access policies across multiple devices from a single interface.

ENHANCE VISIBILITY AND REPORTING

An in-depth view of logs and events provides access policy session details. With reports available through BIG-IQ Centralized Management, BIG-IP APM helps you gain greater visibility into application access and traffic trends, aggregate data for long-term forensics, accelerate incident responses, and identify issues and unanticipated problems before users can experience them.

BIG-IP APM customizes reports with granular data and statistics for intelligent reporting and analysis. Examples include detailed session reports by:

- Access failures
- Users
- Resources accessed
- Group usage
- IP geolocation

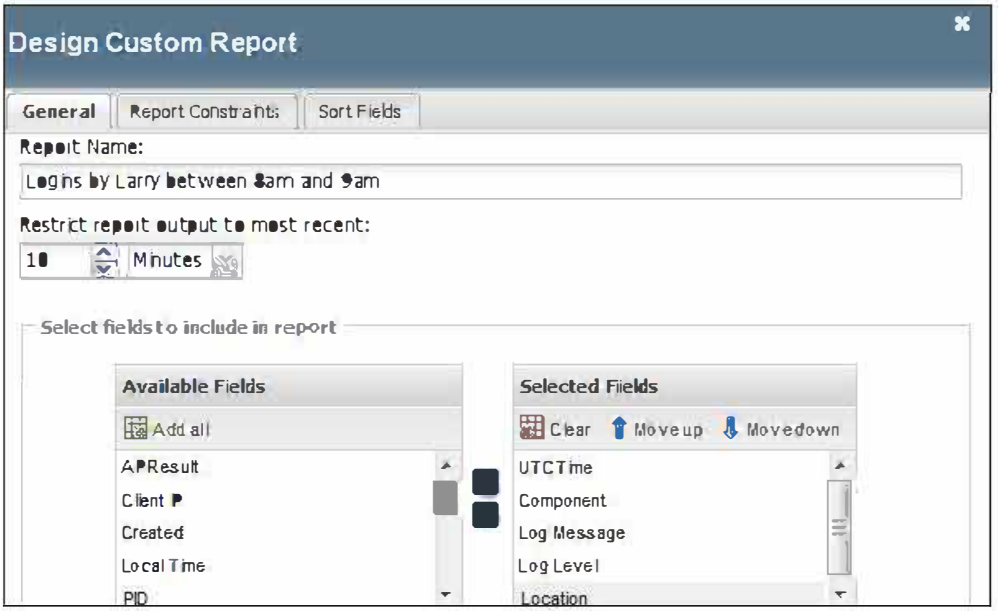


Figure 6: Custom reports provide granular data and statistics for intelligent analysis.

BIG-IP APM integrates with BIG-IQ Centralized Management to provide enhanced visibility through access reports and logs. It delivers analytical reports and logs based on devices and groups, increasing insight into user access and analysis. It also helps you take quick action if required, including the termination of specific access sessions. In addition, it provides a CSV export of BIG-IP APM report data, so it's accessible for customized reports.

BIG-IQ Centralized Management's customized dashboard helps to better envision trends and relationship contexts. This improves response time should issues arise. This holistic view of application and network access enables a better understanding of the effectiveness of established access policies, makes it easier to locate and address weak points, and enhance responses to issues and concerns.

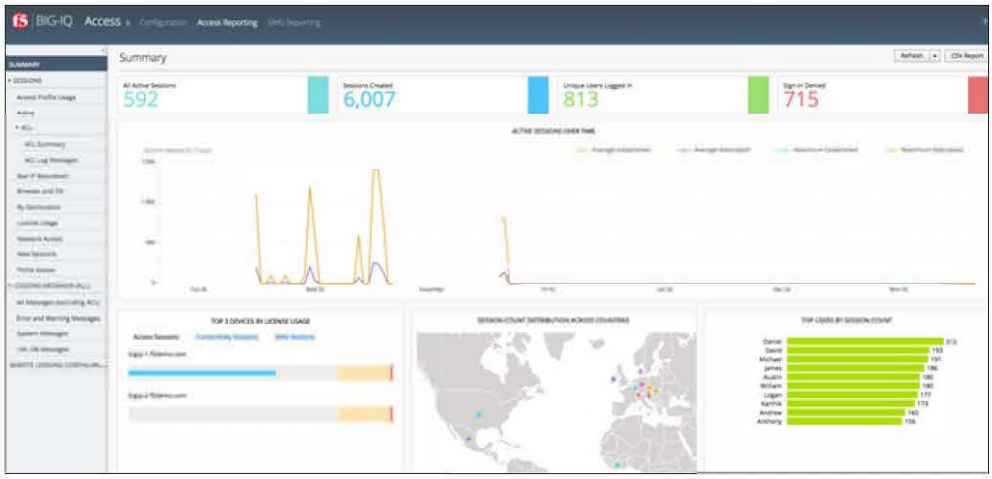


Figure 7: The BIG-IQ Centralized Management comprehensive dashboard for BIG-IP APM helps you better view trends and relationship contexts.

The access policy dashboard on the BIG-IP system also provides a fast overview of access health. You can view the default template of active sessions, network access throughput, new sessions, and network access connections, or create customized views using the dashboard windows chooser. By dragging and dropping the desired statistics onto the windowpane, you gain a real-time understanding of access health.

UNPARALLELED FLEXIBILITY, HIGH PERFORMANCE, AND SCALABILITY

BIG-IP APM delivers flexible application, network, and cloud access, keeping your users productive and enabling your organization to scale quickly and cost-effectively.

BIG-IP APM can be deployed a variety of ways to address your specific access needs. BIG-IP APM may be:

- Deployed as an add-on module for BIG-IP LTM to protect public-facing applications
- Delivered as a standalone BIG-IP appliance or as standalone F5 VIPRION® chassis
- Included with a BIG-IP LTM Virtual Edition (VE) to deliver flexible application access in virtualized environments

- Run on high-end Virtual Editions and high-performance Virtual Editions
- Offered on a Turbo SSL platform

In addition to being licensed for these platforms, BIG-IP APM may also be licensed as part of the Best bundle in F5's Good-Better-Best offering, as part of F5 Enterprise Licensing Agreement (ELA) for BIG-IP VEs, and subscription licensing models.

BIG-IP APM supports F5 Virtual Clustered Multiprocessing™ (vCMP). The vCMP hypervisor provides the ability to run multiple instances of BIG-IP APM, resulting in multi-tenancy and effective separation. With vCMP, network administrators can virtualize while achieving a higher level of redundancy and control.

BIG-IP APM offers SSL offload at network speeds and supports up to 3,000 logins per second. For organizations with an ever-growing base of web application users, this solution scales quickly and cost-effectively.

BIG-IP APM use is based on two types of user sessions: access sessions and concurrent connection use (CCU) sessions. Access sessions apply to authentication sessions, IAP, VDI, and similar situations. CCU is applicable for network access, such as full VPN access, application tunnels, or web access. The BIG-IP platform and the VIPRION platform—both of which support BIG-IP APM—handle exponentially more access sessions than CCU sessions in use cases such as authentication, SAML, SSO, and forward proxy. If you intend to use BIG-IP APM for authentication, VDI, and similar scenarios, supported sessions on VIPRION can reach 2 million, and the BIG-IP platform can support up to 1 million.

BIG-IP APM Features

Whether running as a standalone, a bundled BIG-IP platform module, or on a VIPRION chassis blade, BIG-IP APM is based on the intelligent, modular F5 TMOS® operating system that delivers insight, flexibility, and control to help you better enable application, network, and cloud access.

BIG-IP APM FEATURES INCLUDE:

Access Policies

- Full proxy
- Granular access policy enforcement
- Creating and managing identity- and context-aware policies
- Policy routing
- Identity- and context-based authorization with dynamic L4/L7 ACLs
- Risk-based access leveraging third-party UEBA and risk engines (HTTP Connector)
- Configurable timeouts
- DNS cache/proxy support
- IP geolocation agent (in VPE)
- Visual Policy Editor (VPE)
- Compatible with JavaScript Parser ES 6/7

Authentication and Authorization Support

- Bridging modern authentication and authorization (SAML, OAuth/OIDC) and classic authentication and authorization methods
- Authentication methods: form, certificate, Kerberos SSO, SecurID, basic, RSA token, smart card, N-factor
- Support for SAML-based authentication using BIG-IP Edge Client and F5 Access for Android and iOS
- Step-up authentication support
- Support for SAML-artifact binding
- Support for SAML ECP profile support
- Support for OAuth 2.0 authorization protocol
- Multi-factor authentication (MFA) via one-time password (OTP) solution
- Supports Google reCAPTCHA v2 for authentication and contextual authentication
- AAA server authentication and high-availability
- User credential protection
- Integrates with third-party multi-factor authentication (MFA) solutions, including Duo (Cisco) and Microsoft Azure Active Directory

Identity Aware Proxy / Zero Trust Application Access

- Support for Identity Aware Proxy (IAP) enabling zero trust application access
- Enables per-request application access
- Continuous endpoint integrity and security checks
- Integrates with Microsoft Azure Active Directory Conditional Access

Identity Federation and SSO

- SAML 2.0 identity federation support
- Simplified identity federation for applications with multi-valued attributes
- Dynamic "webtops," based on user identity
- Microsoft Identity Platform 2.0 support
- SSO support for classic authentication (Kerberos, header- based, etc.), credential caching, OAuth 2.0, SAML 2.0, and FIDO2 (U2F)
- Integrates with third-party SSO solutions
- Credential caching and proxy for SSO
- Integrates with third-party Identity-as-a-Service (IDaaS) solutions, including Microsoft Azure Active Directory and Okta

Remote Access

- Enables zero trust application access
- SSL VPN remote access
- Always connected access
- Establish an always-on VPN tunnel (with Windows OS login and BIG-IP Edge Client for Windows)
- Site-to-site IPsec encryption
- Application tunnels
- Support for endpoint security and VPN without web browser plug-ins
- DTLS 2.0 mode for delivering and securing applications
- Support for dynamic split tunneling

API Protection

- API protection and authorization
- Supports and imports OpenAPI 3.0 (Swagger) files
- Supports configuration of quotas, allow-lists, and deny-lists for rate limiting API requests

Simplified Administrative Experience

- Access Guided Configuration (AGC)
- Simplified guided access support for classic applications, including SAP ERP, Oracle PeopleSoft, Oracle E-Business Suite (EBS), and Oracle JD Edwards
- External logon page support
- Landing URI variable support
- IPv6 ready
- Style sheets for customized logon page
- Health check monitor for RADIUS accounting
- AES128-GCM encryption

Scalability

- Scales up to 2 million concurrent access sessions

Growing Ecosystem

- Broad client platform support (see F5 BIG-IP APM Client Compatibility Matrices for each BIG-IP release)
- Robust web browser support (see F5 BIG-IP APM Client Compatibility Matrices for each release)
- Support for Identity-as-a-Service (IDaaS), including Microsoft Azure Active Directory and Okta
- BIG IP Edge Client and F5 Access integrate with VMware Workspace ONE (AirWatch), Microsoft Intune and IBM MaaS360
- Seamlessly integrates with third-party MFA, including Duo (Cisco)
- OIDC protocol support for Duo (Cisco) MFA
- Integrates with leading IAM vendor products (Microsoft, Okta, Ping Identity)
- Integrates with Microsoft Azure AD Conditional Access
- Windows machine certificate support
- Windows Credential Manager integration

Reporting and Visibility

- Export and import of access policies via BIG-IQ Centralized Management
- Centralized advanced reporting with Splunk

Virtual Appliance

- VMware Horizon View 7.13 and Horizon 8.0 support

Additional F5 Support

- vCMP
- F5 iRules® scripting language
- Access control support to BIG-IP LTM virtual server

F5 BIG-IP Platforms

Please refer to the BIG-IP System Hardware, VIPRION, and Virtual Edition data sheets for more details. For information about specific module support for each platform, see the latest release notes on AskF5. For the full list of supported hypervisors, refer to the VE Supported Hypervisors Matrix. F5 platforms can be managed via a single pane of glass with BIG-IQ Centralized Management.

BIG-IP iSeries Appliances

BIG-IP Virtual Editions

VIPRION Chassis

F5 Support Services

F5 Support Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Support Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Support Services, contact consulting@f5.com or visit f5.com/services/support.

To learn more about BIG-IP APM, visit f5.com/apm.