PT APPLICATION FIREWALL PRO

راهکار پیشرفته حفاظت از برنامه‌های وب و API

معرفی، معماری، قابلیت‌ها و بررسی فنی در مقایسه با راهکارهای Enterprise WAF

نگارش ۱.۳ شهریور ۱۴۰۵

SAFE NEST
COMMUNICATION
INTERNATIONAL

آدرس : تهران – خیابان شهید استاد مطهری – خیابان شهید سرافراز – پلاک ۹ طبقه ۳ واحد غربی
تلفن : ۴۲۰۷۰۰۰۰(۹۸+)
ایمیل : info@safenest.ir (https://www.safenest.ir)

مقدمه

با گسترش سرویس‌های مبتنی بر وب، سامانه‌های سازمانی، پرتال‌های خدماتی، بانکداری الکترونیکی، تجارت الکترونیکی و APIها، بخش قابل توجهی از سطح حمله سازمان‌ها از لایه شبکه به لایه Application منتقل شده است. در چنین شرایطی استفاده از Firewall و Intrusion Prevention System به تنهایی نمی‌تواند امنیت برنامه‌های وب را تضمین کند، زیرا بسیاری از حملات جدید در قالب درخواست‌های کاملاً معتبر HTTP و HTTPS به سمت Application ارسال می‌شوند و تشخیص آنها نیازمند تحلیل عمیق ساختار Request، Session، رفتار کاربر و منطق برنامه است.

Web Application Firewall یا WAF با قرار گرفتن در مسیر ارتباط کاربران با Web Application، ترافیک لایه Application را تحلیل کرده و تلاش می‌کند درخواست‌های مخرب را پیش از رسیدن به سرویس اصلی شناسایی و متوقف کند. یک WAF مدرن علاوه بر Signatureهای متداول باید توانایی تحلیل رفتاری، یادگیری الگوی Application، حفاظت از API، مقابله با Bot، کنترل حملات Application Layer DDoS و شناسایی حملاتی را داشته باشد که هنوز Signature مشخصی برای آنها ایجاد نشده است.

PT Application Firewall PRO یا PT AF PRO محصول شرکت Positive Technologies برای حفاظت از Web Applicationها و APIها است. این محصول برای مقابله با حملات شناخته‌شده و همچنین حملات پیچیده و Zero-Day طراحی شده و از ترکیبی از روش‌های تشخیص مبتنی بر Rule، تحلیل رفتار، Application Profiling، Machine Learning و Correlation استفاده می‌کند.

PT AF PRO تنها به مسدودسازی حملاتی مانند SQL Injection یا Cross-Site Scripting محدود نیست. معماری محصول به گونه‌ای طراحی شده که بتواند لایه‌های مختلفی از امنیت Application را پوشش دهد؛ از تحلیل Request و Response گرفته تا شناسایی Bot، کنترل رفتار کاربران، مقابله با DDoS ۷L و حفاظت از آسیب‌پذیری‌های Application تا زمانی که اصلاح آنها در Source Code امکان‌پذیر شود.

از دیدگاه معماری نیز PT AF PRO یک راهکار قابل توسعه برای محیط‌های Enterprise است و می‌تواند متناسب با اندازه سازمان و میزان ترافیک، از یک استقرار نسبتاً ساده تا معماری Cluster و محیط‌های توزیع‌شده مورد استفاده قرار گیرد. معماری Container-based و قابلیت توسعه منابع پردازشی، امکان استفاده از محصول در سامانه‌های پرترافیک و محیط‌های دارای چندین Application را فراهم می‌کند. Positive Technologies همچنین برای AF PRO قابلیت‌هایی مانند Multitenancy، مدیریت متمرکز و توسعه ظرفیت پردازشی را در نظر گرفته است

[تصویر شماره ۱]

جایگاه PT AF PRO در معماری امنیت Application

هدف اصلی PT AF PRO ایجاد یک لایه حفاظتی میان کاربران و سرویس‌های Application است. در این معماری، درخواست‌های HTTP و HTTPS پیش از رسیدن به Application مورد بررسی قرار می‌گیرند و WAF درباره عبور، ثبت، محدودسازی یا مسدودسازی آنها تصمیم می‌گیرد.

برخلاف Firewallهای شبکه که تصمیم‌گیری آنها عمدتاً بر مبنای مشخصاتی مانند Source، Destination، Port، Protocol و اطلاعات Connection انجام می‌شود، WAF محتویات و ساختار ارتباط Application را بررسی می‌کند. برای مثال دو Request ممکن است از نظر IP، Port و Protocol کاملاً مشابه باشند، اما یکی یک درخواست قانونی به Application و دیگری شامل SQL Injection، XSS، Command Injection یا تلاش برای سوءاستفاده از یک API باشد.

PT AF PRO برای حل این مسئله از یک مدل حفاظتی چندلایه استفاده می‌کند. درخواست ورودی می‌تواند از چندین مکانیزم Detection عبور کند و نتیجه تحلیل این مکانیزم‌ها برای تشخیص دقیق‌تر حملات مورد استفاده قرار گیرد.

یکی از مهم‌ترین اجزای این معماری، Application Profiling است. سیستم با تحلیل ترافیک Application می‌تواند الگوی متعارف Requestها را شناسایی کند و Requestهایی را که از رفتار معمول Application فاصله دارند به عنوان Anomaly بررسی کند. این قابلیت اهمیت زیادی در مقابله با حملاتی دارد که هنوز Rule یا Signature مشخصی برای آنها در دسترس نیست. Positive Technologies این قابلیت Machine Learning و Application Profiling را یکی از روش‌های AF PRO برای شناسایی حملات Zero-Day معرفی می‌کند

در کنار این مکانیزم، Ruleها و Signatureهای امنیتی نیز برای شناسایی الگوهای شناخته‌شده حمله مورد استفاده قرار می‌گیرند. ترکیب Signature Detection و Behavioral Analysis باعث می‌شود محصول تنها وابسته به یک روش شناسایی نباشد.

Correlation نیز بخش مهم دیگری از معماری حفاظتی است. در حملات پیچیده ممکن است هر Request به تنهایی نشانه قطعی یک حمله نباشد، اما مجموعه‌ای از رخدادهای مرتبط در یک بازه زمانی بتواند رفتار مهاجم را مشخص کند. Correlation امکان مرتبط کردن چنین Eventهایی را فراهم می‌کند و دید دقیق‌تری نسبت به Attack Sequence ایجاد می‌کند.

PT AF PRO همچنین امکان تحلیل Session و فعالیت کاربران را فراهم می‌کند. در چنین مدلی تصمیم امنیتی صرفاً بر اساس یک Packet یا Request منفرد گرفته نمی‌شود، بلکه رفتار User یا Session نیز می‌تواند بخشی از فرآیند تشخیص باشد.

در نتیجه می‌توان معماری حفاظتی محصول را به چند لایه اصلی تقسیم کرد:

- لایه دریافت و پردازش HTTP/HTTPS
- لایه Signature و Rule-Based Detection
- لایه Application Profiling و Machine Learning
- لایه Behavioral Analysis
- لایه User و Session Analysis
- لایه Correlation
- لایه Policy Enforcement
- لایه Event Management و Monitoring

[تصویر شماره ۲]

حفاظت فراتر از WAF سنتی

نسل اولیه Web Application Firewallها عمدتاً مبتنی بر Signature بودند. در این روش WAF ساختار Request را با مجموعه‌ای از الگوهای از پیش تعریف‌شده مقایسه می‌کرد و در صورت مشاهده Pattern شناخته‌شده حمله، Request را مسدود می‌کرد.

این روش همچنان یکی از بخش‌های مهم امنیت Application است اما برای مقابله با تهدیدات امروزی کافی نیست. مهاجم می‌تواند Payload را تغییر دهد، Encodingهای متفاوتی استفاده کند، حمله را در چند مرحله اجرا کند یا از یک آسیب‌پذیری جدید استفاده کند که هنوز Signature آن تولید نشده است , PT AF PRO برای کاهش این محدودیت از چندین مکانیزم مکمل استفاده می‌کند :

- Application Profiling
  - با تحلیل Requestهای معتبر، ساختار متعارف ارتباط کاربران با Application مشخص می‌شود. انحراف معنی‌دار از این Profile می‌تواند به عنوان نشانه‌ای از رفتار غیرعادی مورد بررسی قرار گیرد.
- Machine Learning
  - Machine Learning برای تحلیل الگوهای Application و کاربران استفاده می‌شود و در تشخیص Anomalyها و حملاتی که Rule مشخصی برای آنها وجود ندارد نقش دارد. این روش خصوصاً در مقابل برخی Zero-Day Attackها اهمیت پیدا می‌کند.
- Automatic Vulnerability Detection
  - PT AF PRO می‌تواند با تحلیل HTTP Responseها برخی نشانه‌های آسیب‌پذیری Application را تشخیص دهد. این رویکرد باعث می‌شود WAF علاوه بر مشاهده Request مهاجم، اطلاعات حاصل از رفتار Application را نیز در تحلیل خود مورد استفاده قرار دهد.

- Virtual Patching
  - در بسیاری از سازمان‌ها اصلاح یک آسیب‌پذیری در Application بلافاصله امکان‌پذیر نیست. ممکن است Source Code متعلق به پیمانکار باشد، Application قدیمی باشد، انجام Patch نیازمند آزمون‌های طولانی باشد یا اعمال تغییر باعث اختلال در سرویس حیاتی شود.
  - Virtual Patching در چنین شرایطی یک لایه دفاعی موقت ایجاد می‌کند تا مسیر Exploit شدن آسیب‌پذیری در WAF مسدود شود؛ بدون آنکه الزاماً در همان لحظه تغییری در Application اصلی ایجاد شود.
  - Positive Technologies برای این حوزه ماژول P-Code را نیز معرفی کرده است. این ماژول با تحلیل Source Code برنامه، آسیب‌پذیری‌ها را شناسایی کرده و امکان ایجاد حفاظت هدفمند در برابر Exploit آنها را فراهم می‌کند
- Client-Side Protection
  - تمام حملات Application الزاماً مستقیماً سرور را هدف قرار نمی‌دهند. برخی حملات کاربری که Browser را هدف قرار می‌دهند نیز می‌توانند منجر به سرقت Session، اطلاعات حساس یا اجرای عملیات غیرمجاز شوند.
  - PT برای این حوزه WAF.js را ارائه کرده است. این Client Module برای مقابله با تهدیداتی از جمله XSS، DOM XSS، DOM Clobbering و CSRF طراحی شده است
- Malware Inspection
  - Web Applicationها معمولاً امکان Upload و Download فایل دارند و همین قابلیت می‌تواند به یک مسیر انتقال Malware تبدیل شود. ماژول M-Scan در اکوسیستم PT AF برای تحلیل فایل‌های آپلود و دانلودشده طراحی شده و Positive Technologies اعلام می‌کند این ماژول امکان استفاده از چندین Antivirus Engine را فراهم می‌کند.


positive technologies
SECURING A SAFER TOMORROW
لایه‌های حفاظتی PT AF PRO
حفاظت هوشمند از برنامه‌های کاربردی در برابر تهدیدات مدرن
PEOPLE TECHNOLOGIES A SAFER TOMORROW
PT
DETECT ANALYZE PROTECT STAY AHEAD
Security Layer | وظیفه | نمونه تهدید | مکانیزم PT AF PRO
Signature Detection | شناسایی الگوهای شناخته‌شده حمله | SQL Injection، XSS، Path Traversal | Rule-Based Detection و Signature Engine
Machine Learning | تحلیل ناهنجاری و شناسایی رفتار غیرعادی | Zero-Day Attack، Anomalous Requests | ML Models و Behavioral Analysis
Application Profiling | مدل‌سازی رفتار عادی برنامه | Requestهای خارج از الگوی معمول، | Application Profile و Baseline Analysis
User Tracking | ردیابی رفتار کاربر و Session | Brute Force، Credential Abuse | Session Analysis و User Behavior Monitoring
Correlation | ارتباط دادن رخدادهای پراکنده | Attack Sequence، Multi-Step Attacks | Correlation Engine و Event Linking
WAF.js | حفاظت سمت کاربر و Browser | DOM XSS، CSRF، DOM Clobbering | Client-Side Protection Module
M-Scan | تحلیل فایل‌های Upload و Download | Malware Upload، Infected Files | File Inspection و Multi-Engine Scanning
P-Code | ایجاد Virtual Patch بر اساس تحلیل کد | Exploitation of Known Vulnerabilities | Source Code Analysis و Virtual Patching
L7 DDoS Protection | مقابله با DoS در لایه Application | HTTP Flood، Resource Exhaustion | Rate Analysis، User Profiling و Traffic Control
Bot Protection | تشخیص و کنترل Botهای مخرب | Credential Stuffing، Scraping، Automated Abuse | Bot Detection، Client Verification و Behavior Analysis
POSITIVE TECHNOLOGIES
APPLICATION SECURITY / HIGHER CONFIDENCE / STRONGER BUSINESSES
SECURITY WITHOUT LIMITS

[جدول شماره ۱]

معماری استقرار PT AF PRO

یکی از نقاط مهم در طراحی WAF، روش قرار گرفتن آن در معماری شبکه است. انتخاب Deployment Mode باید با توجه به ساختار شبکه، حساسیت Application، امکان تغییر Routing، الزامات High Availability و این موضوع انجام شود که آیا WAF صرفاً باید ترافیک را Monitor کند یا باید امکان مسدودسازی مستقیم حملات را نیز داشته باشد.

PT Application Firewall سه مدل اصلی Integration را ارائه می‌کند:

- Reverse Proxy
  - Reverse Proxy متداول‌ترین مدل استفاده عملیاتی از WAF است. در این معماری Client به جای برقراری ارتباط مستقیم با Web Server، ارتباط خود را با WAF برقرار می‌کند. PT AF PRO Request را دریافت، بررسی و در صورت مجاز بودن به Backend Server منتقل می‌کند ,
  - این معماری امکان کنترل کامل Request و Response و مسدودسازی مستقیم حملات را فراهم می‌کند. در ارتباط HTTPS نیز WAF می‌تواند در نقطه مناسب فرآیند رمزگشایی و تحلیل Security Policy را انجام دهد.
  - استقرار Reverse Proxy علاوه بر Visibility بیشتر، امکان اعمال Policy دقیق‌تر روی Applicationها را فراهم می‌کند و Positive Technologies نیز این روش را متداول‌ترین سناریوی Integration محصول معرفی می‌کند.

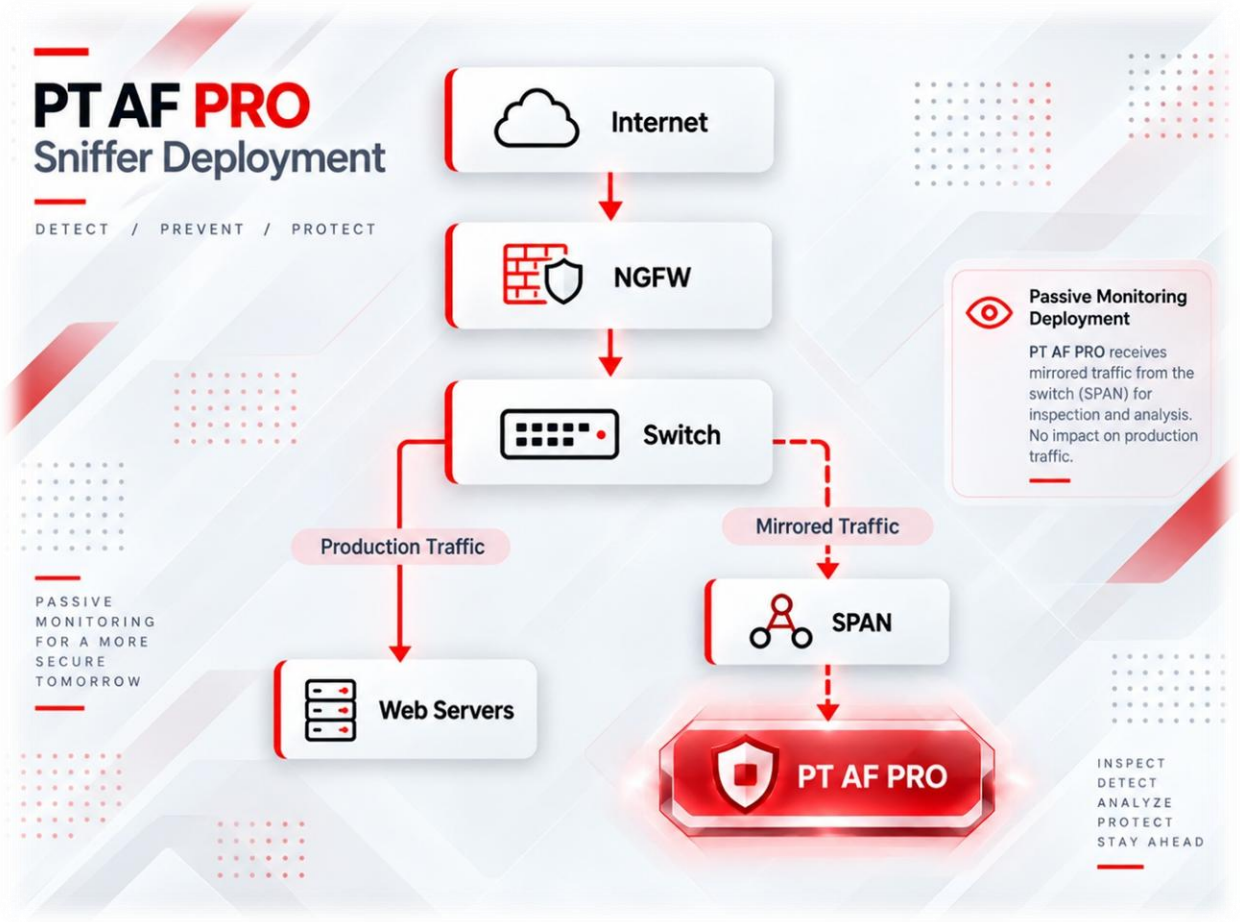
[تصویر شماره ۳]

- Transparent Proxy
  - در Transparent Proxy محصول در مسیر ارتباط Client و Server قرار می‌گیرد اما می‌تواند در قالب یک Bridge ۲L عمل کند.مزیت مهم چنین معماری‌ای کاهش نیاز به تغییر گسترده در IP Addressing یا Routing موجود است. این روش برای سازمان‌هایی اهمیت دارد که قرار دادن WAF در مسیر ترافیک ضروری است اما ایجاد تغییرات گسترده در ساختار شبکه مطلوب نیست.

[تصویر شماره ۴]

- Sniffer Mode و انتخاب مدل مناسب استقرار
  - Sniffer Mode با دو مدل قبلی تفاوت اساسی دارد ؛ در این معماری PT AF PRO الزاماً در مسیر مستقیم ارتباط Client و Application قرار نمی‌گیرد. یک کپی از Traffic، معمولاً از طریق SPAN یا Traffic Mirroring، در اختیار WAF قرار می‌گیرد و سیستم ترافیک Application را تحلیل می‌کند.
  - مزیت مهم Sniffer Mode آن است که می‌توان WAF را بدون ایجاد تغییر اساسی در Traffic Path و با ریسک عملیاتی پایین وارد شبکه کرد.
  - این مدل برای مرحله Pilot، شناخت Application، بررسی Eventها، تنظیم Security Policy و ارزیابی اولیه رفتار محصول بسیار مفید است.

- اما تفاوت بنیادی آن با Reverse Proxy یا Transparent Proxy در این است که PT AF در مسیر مستقیم Traffic قرار ندارد. بنابراین Sniffer را باید عمدتاً یک Deployment Mode برای Visibility، تحلیل و Detection در نظر گرفت، در حالی که Inline Deployment برای Enforcement و جلوگیری مستقیم از عبور Request مخرب مناسب‌تر است. Positive Technologies نیز Sniffer Mode را به عنوان تحلیل کپی ترافیک دریافت‌شده از SPAN Port معرفی می‌کند.



[تصویر شماره ۵]

روی مسیر Web Server عبارت Production Traffic و روی مسیر PT AF عبارت Mirrored Traffic نوشته شود.

انتخاب Deployment Mode

هیچ یک از سه روش استقرار را نمی‌توان به صورت مطلق برای همه سازمان‌ها بهترین گزینه دانست. انتخاب معماری وابسته به اهداف پروژه است. اگر هدف اصلی در مرحله اول مشاهده ترافیک، شناسایی Application Behavior و تنظیم Policy بدون ایجاد تغییر در مسیر Production باشد، Sniffer Mode می‌تواند گزینه مناسبی برای شروع پروژه باشد.

اگر هدف اعمال کامل Security Policy و مسدودسازی Real-Time حملات باشد، Reverse Proxy معمولاً معماری کامل‌تری در اختیار تیم امنیت قرار می‌دهد.

Transparent Proxy نیز در محیط‌هایی ارزشمند است که Inline Inspection مورد نیاز است ولی سازمان تمایل دارد تغییرات Routing و معماری شبکه را به حداقل برساند.

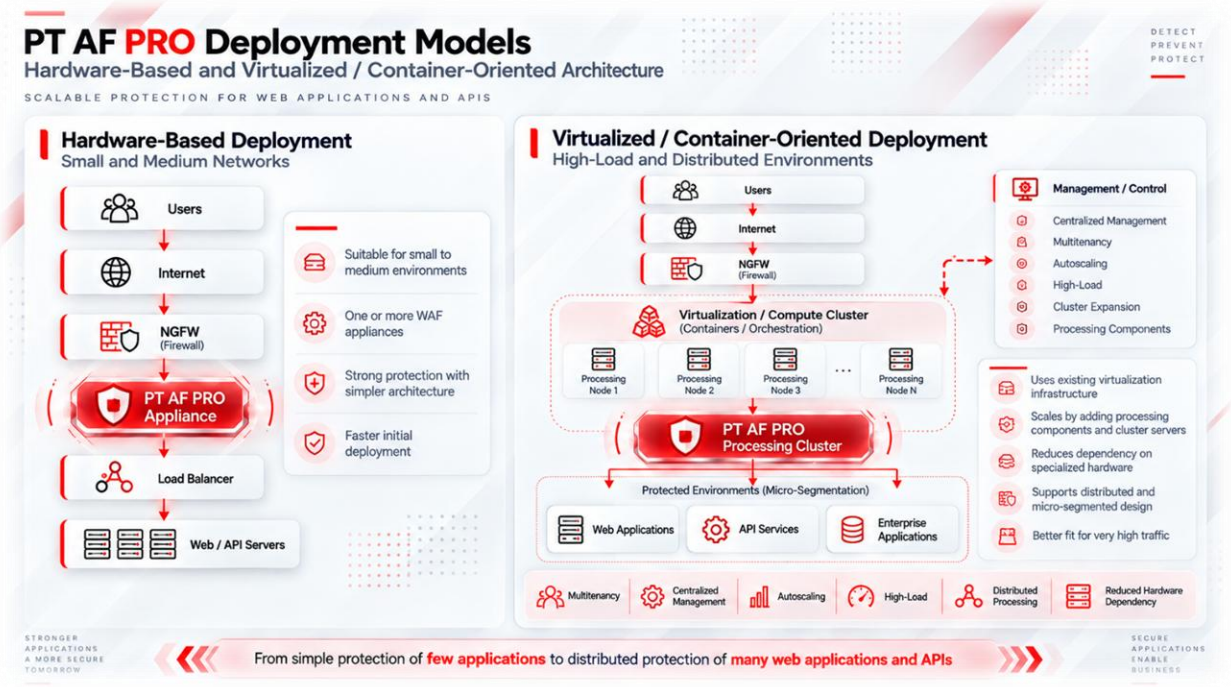
ویژگی	Sniffer	Reverse Proxy	Transparent Proxy
قرارگیری Inline	خیر	بله	بله
امکان تحلیل Traffic	بله	بله	بله
قابلیت Blocking مستقیم	خیر	بله	بله
نیاز به تغییر معماری شبکه	کم	متوسط تا زیاد	کم تا متوسط
مناسب برای Pilot	بسیار مناسب	مناسب	مناسب
مناسب برای Production Protection	محدود	بسیار مناسب	مناسب
پیچیدگی Deployment	پایین	متوسط	متوسط
تأثیر بالقوه بر Traffic Path	تقریباً بدون تأثیر	مستقیم در مسیر ترافیک	در مسیر ترافیک با تغییر کمتر

[جدول شماره ۲]

معماری مناسب برای محیط Enterprise

در یک محیط عملیاتی بزرگ، WAF نباید به عنوان یک Server مستقل و منفرد در نظر گرفته شود. Scalability، Availability، Capacity Planning و Failure Handling باید از ابتدای طراحی در معماری لحاظ شوند.

PT AF PRO برای محیط‌های بزرگ از معماری Container-oriented و قابلیت توسعه ظرفیت پردازشی استفاده می‌کند. Positive Technologies در معرفی فعلی محصول بر Multitenancy، Centralized Management، Autoscaling و استفاده در محیط‌های High-Load تأکید می‌کند و برای سناریوهای پرترافیک، امکان افزایش تعداد Processing Componentها و Serverهای Cluster را در نظر گرفته است , این موضوع باعث می‌شود معماری PT AF PRO را بتوان از یک مدل ساده حفاظت از چند Application به یک معماری توزیع‌شده برای محافظت از تعداد زیادی Web Application و API توسعه داد , در حقیقت مدل مبتنی بر سخت افزار و مدل مبتنی بر مجازی سازی انتخابهایی می باشد که PT AF PRO برای طراحی در اختیار ما قرار میدهد , در شبکه های کوچک و متوسط میتوان با استقرار یک یا چند تجهیز به عنوان WAF امنیت خوبی را تامین نمود اما در شبکه های که حجم ترافیک بسیار زیاد است معماری مبتنی بر سخت افزار گران قیمت مناسب نیست و با استفاده از زیرساخت مجازی سازی موجود در سازمان میتوان به صورت میکروسگمنت طراحی مناسبی داشت و ریسکهای ناشی از ترافیک بالا را در چندین لایه مدیریت نمود و وابستگی به تجهیزات خاص را در معماری کاهش داد .



[تصویر شماره ۶]

معماری Cluster، مقیاس‌پذیری و استقرار در محیط‌های Enterprise

مشکل اساسی در بسیاری از سازمانها در ایران تامین تجهیزات گرانقیمت سخت افزاری WAF مانند F۵ یا Fortiweb و نصب آنها در دروازه های ورودی اینترنت به مرکزداده می باشد همچنین سازمانها مجبورند برای HA حداقل ۲ یا ۳ تجهیز تهیه کنند و نگهداری قطعات آنها با شرایط تحریم و مشکلات واردات مانند پاور و ... دشوار و هزینه زا می باشد .

اما همین معماری نیز مشکلات امنیتی دارد زیرا سامانه های زیادی در داخل سازمان وجود دارد که نیازی به اتصال به اینترنت ندارد از سامانه های محرمانه داخلی یا انواع سامانه های عمومی انبار و ... و حتی API های داخلی بین محصولات مختلف سازمان یا بین سازمانی که بدون WAF در سازمان رها شده است و در صورتی که هکر به هر طریق به شبکه داخلی سازمان نفوذ کند به سادگی این سامانه ها را میتواند مورد حمله قرار دهد .

برخی از سازمانها برای رفع این مشکل سامانه های داخلی خود را به پشت WAF متصل به اینترنت منتقل میکنند که با توجه به انواع باگهای امنیتی کشف شده در سالهای اخیر و خطر نفوذ به این تجهیزات از بیرون سازمان ریسک را چند برابر میکنند !

راهکار بهتر میتواند تهیه چندین WAF مستقل برای سامانه های اینترنتی – سامانه های داخلی و APIهای بین سازمانی باشد که این راهکار با توجه به نیاز به قابلیت HA گران تمام میشود ! برای همین راهکار میکروسگمنت بر پایه WAF های مجازی توسط PT بسیار ارزانتر و مناسبتر است ! نه وابستگی به تجهیزات گران وجود دارد و مشکل تامین نه سامانه های داخلی بی دفاع رها میشوند.

یکی از تفاوت‌های مهم میان یک WAF مورد استفاده برای چند سرویس محدود و یک راهکار Enterprise WAF، توانایی آن در توسعه ظرفیت متناسب با رشد تعداد Applicationها و حجم Traffic است. در محیط‌های بزرگ، معماری WAF باید به گونه‌ای طراحی شود که افزایش تعداد کاربران، APIها، Web Applicationها و نرخ Requestها باعث ایجاد یک نقطه گلوگاه در زیرساخت امنیتی نشود.

PT Application Firewall PRO با تمرکز بر محیط‌های High-Load و Distributed طراحی شده و معماری Container-based آن امکان توسعه ظرفیت پردازشی را با افزایش منابع و تعداد Processing Componentها فراهم می‌کند.

در این مدل، افزایش ظرفیت لزوماً به معنای جایگزینی کامل سیستم با یک Appliance بزرگ‌تر نیست. در صورت افزایش Traffic می‌توان Processing Resource بیشتری به مجموعه اضافه کرد و تعداد Handlerهایی را که وظیفه بررسی Traffic را بر عهده دارند افزایش داد.

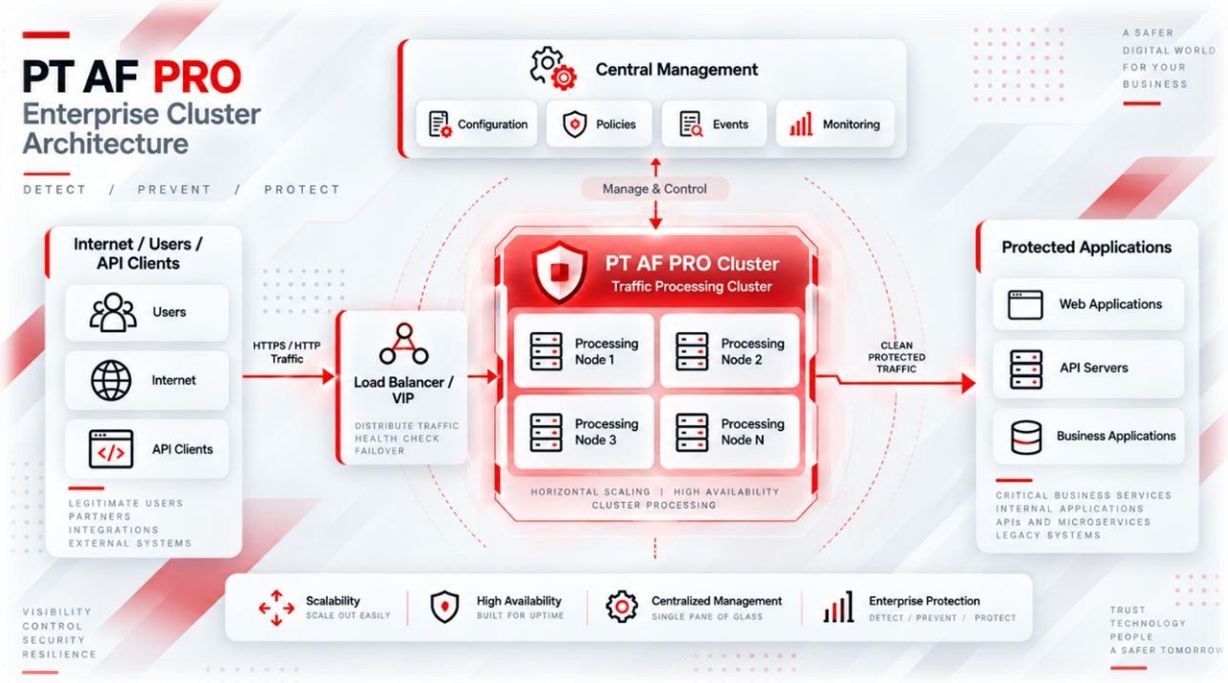
Positive Technologies قابلیت Autoscaling را یکی از ویژگی‌های مهم AF PRO معرفی می‌کند. با افزایش بار، Processing Handlerهای بیشتری می‌توانند برای پاسخ‌گویی به Traffic فعال شوند و در سطح Cluster نیز امکان تغییر تعداد Serverهای مورد استفاده وجود دارد. سازنده همچنین استفاده از PT AF PRO در محیط‌های High-Load با نرخ‌های بیش از ۱۵۰,۰۰۰ Request Per Second و معماری‌های Geographically Distributed را مطرح کرده است.

معماری تفکیک‌شده پردازش و مدیریت

در طراحی Enterprise بهتر است دو وظیفه اصلی WAF از یکدیگر تفکیک شوند:

- Control Plane مسئول مدیریت Configuration، Security Policy، کاربران مدیریتی، Eventها، تنظیمات Application و هماهنگی اجزای سیستم است.
- Traffic Processing Plane وظیفه دریافت و تحلیل Traffic، اجرای Ruleها، Application Profiling، تشخیص حمله و Enforcement سیاست‌های امنیتی را بر عهده دارد.

تفکیک منطقی این وظایف باعث می‌شود افزایش حجم Traffic الزاماً باعث افزایش بار بخش مدیریتی نشود و سازمان بتواند Processing Capacity را متناسب با نیاز خود توسعه دهد.



[تصویر شماره ۷]

مقیاس‌پذیری افقی

Horizontal Scaling در معماری‌های جدید مزیت مهمی نسبت به مدل سنتی Vertical Scaling دارد ,در Vertical Scaling برای افزایش ظرفیت معمولاً باید CPU، RAM یا کل Appliance ارتقا یابد , در Horizontal Scaling ظرفیت با افزودن Processing Node یا Worker جدید افزایش پیدا می‌کند , این موضوع برای سازمان‌هایی که Traffic آنها به تدریج افزایش می‌یابد اهمیت زیادی دارد، زیرا امکان توسعه مرحله‌ای زیرساخت را فراهم می‌کند.

PT AF PRO از معماری Container-based برای افزایش انعطاف‌پذیری در استفاده از منابع بهره می‌گیرد و Positive Technologies این موضوع را به طور مشخص در قابلیت Autoscaling و تغییر تعداد Serverهای Cluster مطرح کرده است

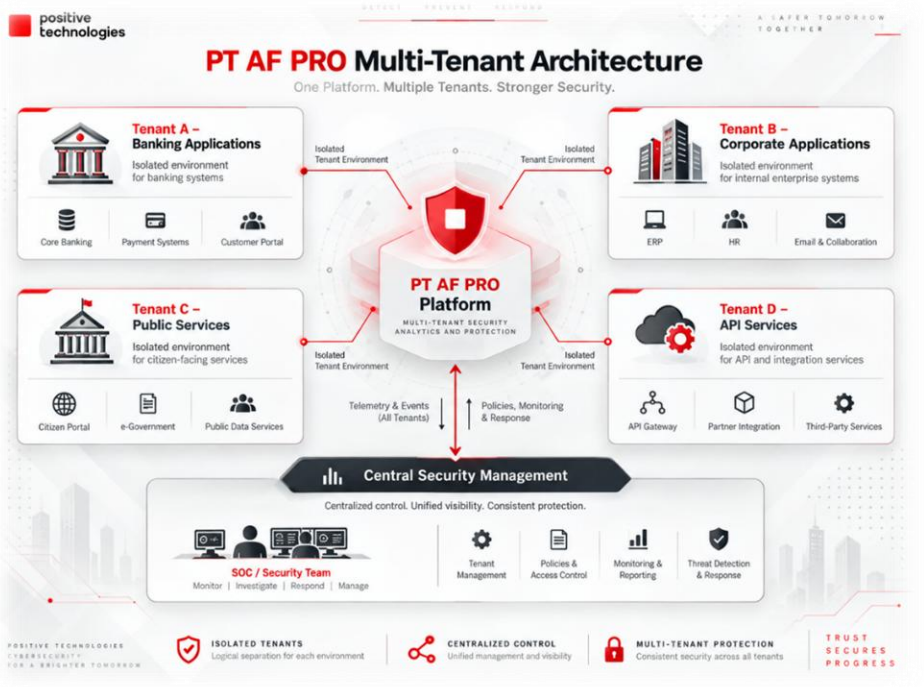
Multitenancy

قابلیت Multitenancy یکی دیگر از ویژگی‌های مهم معماری Enterprise محصول است , در سازمان‌های بزرگ ممکن است یک زیرساخت مرکزی وظیفه حفاظت از Applicationهای چندین شرکت، شعبه یا واحد سازمانی را بر عهده داشته باشد.

Multitenancy امکان ایجاد محدوده‌های منطقی مجزا را در یک Platform مشترک فراهم می‌کند , این معماری به خصوص برای موارد زیر مناسب است:

- Holdingها
- شرکت‌های دارای چند Subsidiary
- Service Providerها
- Data Centerها
- MSSPها
- سازمان‌های دارای چند Business Unit مستقل

Positive Technologies اعلام می‌کند معماری Multitenant محصول امکان حفاظت از ده‌ها شرکت زیرمجموعه در یک سیستم را فراهم می‌کند و Container Architecture باعث جداسازی بهتر بار و منابع میان آنها می‌شود.



[تصویر شماره ۸]

موتور تشخیص حمله و مدل چندلایه Detection

توانایی یک Web Application Firewall را نباید تنها با تعداد Signatureهای آن ارزیابی کرد. حملات Application امروزی می‌توانند با تغییر Payload، Encoding، ساختار Request یا ترکیب چند رفتار مختلف تلاش کنند مکانیزم‌های ساده Signature-Based Detection را دور بزنند , به همین دلیل PT AF PRO از ترکیبی از مکانیزم‌های مختلف برای Detection و Protection استفاده می‌کند.

هدف این معماری ایجاد Defense in Depth در سطح Application است؛ یعنی اگر یک روش تشخیص نتواند یک Request مخرب را شناسایی کند، لایه‌های دیگر امکان تحلیل آن را داشته باشند.

- Signature-Based Detection
  - اولین لایه، شناسایی حملات شناخته‌شده بر اساس Rule و Signature است.
  - این بخش برای مقابله با کلاس بزرگی از حملات شناخته‌شده کاربرد دارد، از جمله:
    - SQL Injection
    - Cross-Site Scripting
    - Command Injection
    - Path Traversal
    - Remote File Inclusion
    - Local File Inclusion
    - Protocol Violation
    - Malicious HTTP Requests
    - و بسیاری از تکنیک‌های مرتبط با OWASP Top ۱۰ و WASC.

PT AF PRO حفاظت از حملات شناخته‌شده در OWASP Top ۱۰ و WASC را جزء قابلیت‌های اصلی خود معرفی می‌کند.

- Application Profiling
  - Application Profiling یک لایه تکمیلی برای Signature Detection است.
  - WAF با مشاهده Traffic قانونی Application می‌تواند الگوی متعارف Requestها را شناسایی کند ,برای مثال:
    - چه URLهایی معمولاً فراخوانی می‌شوند؟
    - چه Parameterهایی در یک Request وجود دارند؟
    - نوع و ساختار مقادیر آنها چیست؟
    - چه Request Methodهایی استفاده می‌شوند؟
    - چه رفتارهایی برای کاربران طبیعی محسوب می‌شود؟

در نتیجه اگر Request جدیدی به شکل معنی‌داری از Profile معمول Application فاصله داشته باشد، سیستم می‌تواند آن را به عنوان Anomaly تحلیل کند.

- Machine Learning
  - Machine Learning در PT AF PRO برای ایجاد و تحلیل Profileهای Application و User مورد استفاده قرار می‌گیرد.
  - اهمیت این مکانیزم در شرایطی مشخص می‌شود که Attack Signature از قبل وجود ندارد.
  - برای مثال اگر مهاجم از یک Zero-Day Vulnerability استفاده کند، ممکن است Payload او با Signatureهای موجود تطابق نداشته باشد، اما رفتار Request نسبت به Traffic عادی Application غیرمعمول باشد.

Positive Technologies اعلام می‌کند Application Profiling مبتنی بر Machine Learning برای شناسایی Anomaly و Blocking حملاتی استفاده می‌شود که هنوز Detection Rule مشخصی برای آنها وجود ندارد.

- User Profiling
  - تحلیل رفتار Application تنها بخشی از مسئله است , رفتار User نیز می‌تواند اطلاعات مهمی در اختیار WAF قرار دهد برای مثال:
    - افزایش ناگهانی نرخ Request
    - تلاش سریع برای دسترسی به URLهای مختلف
    - تعداد زیاد Login Attempt
    - تکرار عملیات مشابه
    - Request Pattern غیرطبیعی
    - Automated Navigation
    - می‌توانند نشانه Bot، Brute Force، Credential Attack یا DDoS ۷L باشند.

PT AF PRO از User Profiling مبتنی بر Machine Learning برای شناسایی برخی از این Anomalyها از جمله Application-Layer DDoS استفاده می‌کند.

- Correlation
  - یک Attack همیشه در قالب یک Request واحد اتفاق نمی‌افتد.
  - مهاجم ممکن است ابتدا Application را شناسایی کند، سپس Endpointهای مختلف را آزمایش کند و در مرحله بعد Exploit را اجرا کند.
  - بررسی هر Event به صورت مستقل ممکن است تصویر کاملی از Attack ایجاد نکند.
  - Correlation Engine می‌تواند Eventهای مرتبطی را که در طول زمان ایجاد شده‌اند به یکدیگر متصل کرده و Attack Chain را بهتر مشخص کند.

Positive Technologies از Correlation و Custom Rule برای مرتبط کردن چند Event منطقی در طول زمان و Audit فعالیت‌های کاربران Web Application استفاده می‌کند.

[تصویر شماره ۸]

- Bot Protection، API Security و مقابله با Application-Layer DDoS
  - حفاظت از Applicationهای امروزی دیگر تنها به تشخیص SQL Injection و XSS محدود نمی‌شود.
  - افزایش استفاده از API، Mobile Application و Automated Services باعث شده حجم زیادی از Traffic وب توسط Software Clientها ایجاد شود.
  - این Clientها می‌توانند قانونی یا مخرب باشند.
  - Search Engineها، Monitoring Systemها و Integration Serviceها نمونه Botهای قانونی هستند.
  - در مقابل مهاجمان می‌توانند از Bot برای فعالیت‌هایی مانند:
    - Credential Stuffing
    - Brute Force
    - Web Scraping
    - Account Enumeration
    - Automated Exploitation
    - Content Harvesting
    - Application-Layer DDoS

استفاده کنند.

- Bot Protection
  - یکی از چالش‌های مهم در Bot Protection تشخیص تفاوت میان Human User، Legitimate Bot و Malicious Bot است.
  - Block کردن ساده تمام Automated Traffic راهکار مناسبی نیست، زیرا تعداد زیادی از سرویس‌های قانونی نیز به صورت Automated فعالیت می‌کنند.
  - PT AF PRO برای مقابله با Botها از تحلیل Behavior و مکانیزم‌های مختلف تشخیص Client استفاده می‌کند.

Positive Technologies به طور مشخص اعلام می‌کند AF PRO قابلیت مقابله با Botهای پیشرفته‌ای را نیز دارد که قادر به اجرای JavaScript و شبیه‌سازی Browser هستند.

[تصویر شماره ۹]

- API Security
  - در معماری‌های جدید بخش قابل توجهی از ارتباط میان سیستم‌ها توسط API انجام می‌شود.
  - Mobile Applicationها، Microserviceها، Business Integrationها و Cloud Serviceها برای تبادل اطلاعات از API استفاده می‌کنند.
  - در نتیجه API عملاً به یکی از مهم‌ترین Attack Surfaceهای سازمان تبدیل شده است.
  - WAF برای حفاظت مؤثر از این محیط باید بتواند علاوه بر URL و HTTP Request، رفتار Client، نرخ فراخوانی، پارامترها و ساختار ارتباط با Application را نیز بررسی کند.
  - قابلیت‌های Protection، Application Profiling، User Profiling، Rate Control و Detection Engineهای PT AF PRO می‌توانند در حفاظت از API Endpointها نیز مورد استفاده قرار گیرند.

- در طراحی Policy برای API معمولاً موارد زیر اهمیت دارند:
  - Request Method
  - URL و Endpoint
  - Parameter
  - Content Type
  - Authentication Behavior
  - Request Rate
  - Response Behavior
  - User یا Client Profile
  - Application-specific Rules

PT AF PRO به طور مشخص به عنوان یک WAF برای حفاظت مستمر از Web Application و API معرفی می‌شود.

- Application-Layer DDoS
  - در Network DDoS معمولاً هدف اشباع Bandwidth یا Network Infrastructure است.
  - اما Application-Layer DDoS می‌تواند با تعداد Request بسیار کمتر، منابع Application را مصرف کند.
  - برای مثال یک Request ممکن است باعث:
    - Database Query سنگین
    - Search Operation
    - Complex Calculation
    - Session Creation
    - File Generation
    - یا فراخوانی یک API پرهزینه شود.
  - در چنین شرایطی صرفاً بررسی حجم Traffic شبکه برای تشخیص Attack کافی نیست.

PT AF PRO از User Profiling مبتنی بر Machine Learning برای شناسایی رفتارهای Anomalous و تلاش‌های ۷L DDoS استفاده می‌کند.

مدیریت متمرکز، عملیات امنیت و Integration

در یک WAF سازمانی، کیفیت Detection Engine تنها بخشی از نیاز است. محصول باید امکان مدیریت تعداد زیادی Application و Security Policy را نیز در اختیار Security Team قرار دهد.

در یک سازمان بزرگ ممکن است صدها Web Application و API در Data Centerهای مختلف وجود داشته باشند. مدیریت جداگانه WAFها در چنین محیطی باعث افزایش Operational Complexity و احتمال ایجاد Policyهای ناسازگار می‌شود.

PT AF PRO امکان Centralized Management را برای مدیریت Policyها و Ruleهای Protection در Installationهای مختلف در نظر گرفته است. Positive Technologies این قابلیت را راهکاری برای کاهش اختلاف Configuration میان سایت‌ها، افزایش سرعت واکنش و کاهش هزینه عملیاتی مدیریت عنوان می‌کند.

- Centralized Policy Management

در معماری متمرکز، Security Team می‌تواند Policyهای حفاظتی Applicationها را از یک Management Layer کنترل کند ,این موضوع در معماری‌های دارای چند Data Center اهمیت بیشتری پیدا می‌کند.

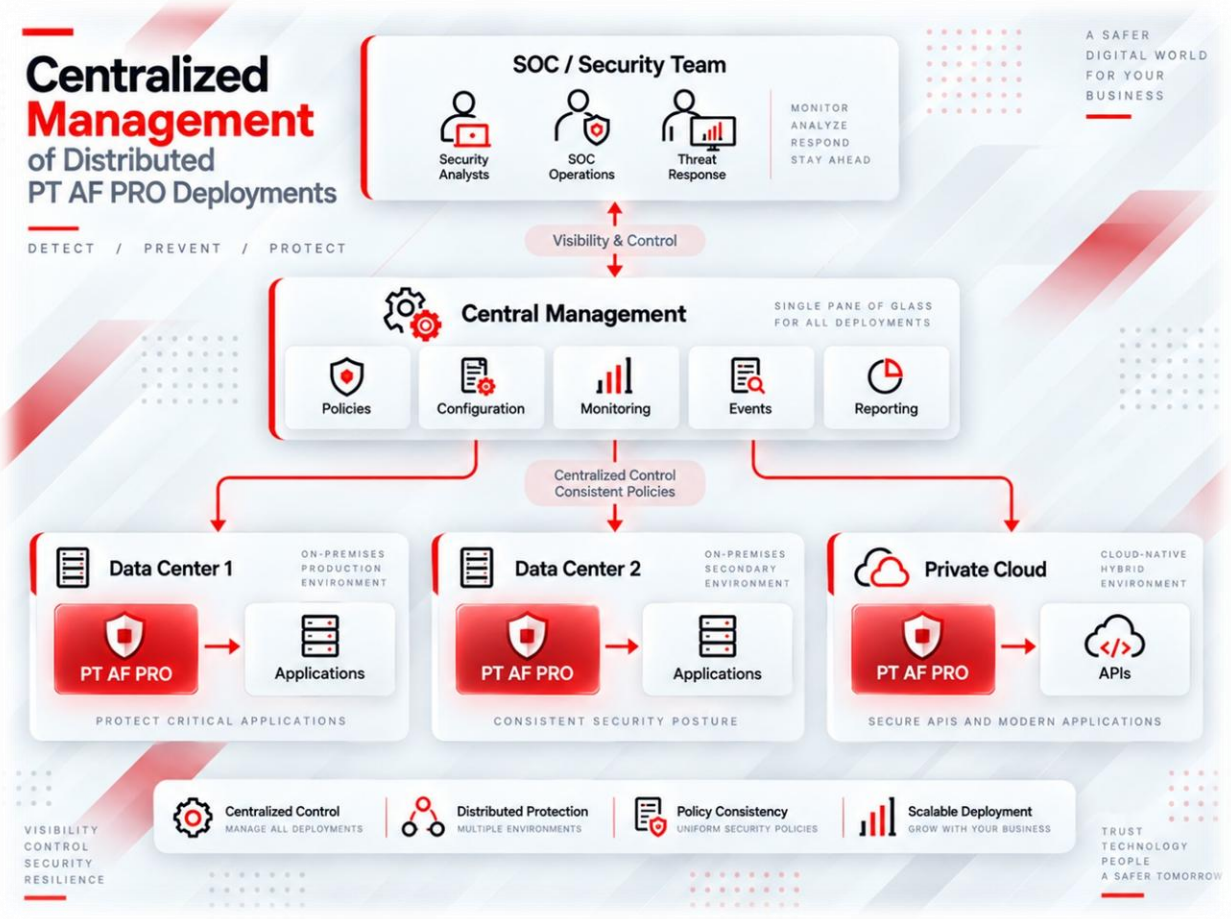
برای مثال یک سازمان ممکن است Applicationهای خود را در:

- Primary Data Center
- Disaster Recovery Data Center
- Private Cloud
- Branch Data Center

مستقر کرده باشد.

در چنین معماری‌ای یکسان بودن Protection Policyها اهمیت زیادی دارد.

Positive Technologies در برنامه قابلیت‌های ۲۰۲۶ خود به Synchronization پارامترهای حفاظتی میان Installationهای PT AF PRO در Data Centerهای مختلف اشاره کرده است.



[تصویر شماره ۱۰]

- Monitoring و Event Analysis

WAF یکی از منابع مهم Telemetry برای SOC محسوب می‌شود , Event ایجادشده توسط WAF می‌تواند اطلاعاتی درباره:

- Source IP
- Target Application
- Requested URL
- Attack Type
- Request Parameter
- User Behavior
- Session
- Security Action
- Attack Sequence

در اختیار تحلیلگر امنیت قرار دهد.

اهمیت این اطلاعات زمانی بیشتر می‌شود که Eventهای WAF در کنار اطلاعات سایر سیستم‌های امنیتی تحلیل شوند.

- Integration با سایر لایه‌های Security

امنیت Application نباید به صورت یک جزیره مستقل طراحی شود.

WAF می‌تواند بخشی از یک معماری چندلایه شامل:

- NGFW
- SIEM
- NDR / NTA
- Sandbox
- Vulnerability Management
- Endpoint Security
- SOC
- Threat Intelligence

باشد.

در اسناد فنی PT نیز معماری Multilayer Protection مطرح شده است که در آن PT AF پس از شناسایی Request مخرب می‌تواند اطلاعات Source تهدید را در اختیار Network Protection System قرار دهد تا محدودسازی در سطح دیگری از شبکه نیز انجام شود.

این رویکرد باعث می‌شود Detection انجام‌شده در Application Layer بتواند در سایر Security Controlها نیز مورد استفاده قرار گیرد.

Integration با چرخه مدیریت Vulnerability

یکی از سناریوهای مهم Integration، ارتباط میان Vulnerability Detection و WAF است. این فرآیند ممکن است روزها یا هفته‌ها طول بکشد. در تمام این مدت Application ممکن است در معرض Exploit قرار داشته باشد.

با استفاده از Virtual Patching می‌توان یک Protection Rule در WAF ایجاد کرد تا تا زمان اصلاح نهایی Application، Exploit مرتبط با Vulnerability مسدود شود.

Positive Technologies برای این سناریو Integration میان Application Security و PT AF را نیز ارائه می‌کند تا آسیب‌پذیری‌های شناسایی‌شده در سطح Firewall در برابر Exploit محافظت شوند.

جایگاه PT AF PRO در برابر Enterprise WAFهای مطرح

بازار Web Application Firewall شامل مجموعه‌ای از راهکارهای Hardware Appliance، Virtual Appliance، Cloud WAF و WAAP Platform است , محصولاتی مانند FortiWeb، F۵ WAF، Advanced WAF، Imperva، Cloudflare WAF و سایر Enterprise Application Security Platformها هر یک معماری و نقاط تمرکز متفاوتی دارند.

بنابراین مقایسه PT AF PRO با رقبا نباید صرفاً بر اساس وجود یا عدم وجود قابلیت‌هایی مانند SQL Injection Protection یا XSS Protection انجام شود , تقریباً تمام Enterprise WAFهای مطرح امروزی این کلاس از حملات را پوشش می‌دهند.

مقایسه واقعی باید در لایه‌های عمیق‌تری انجام شود:

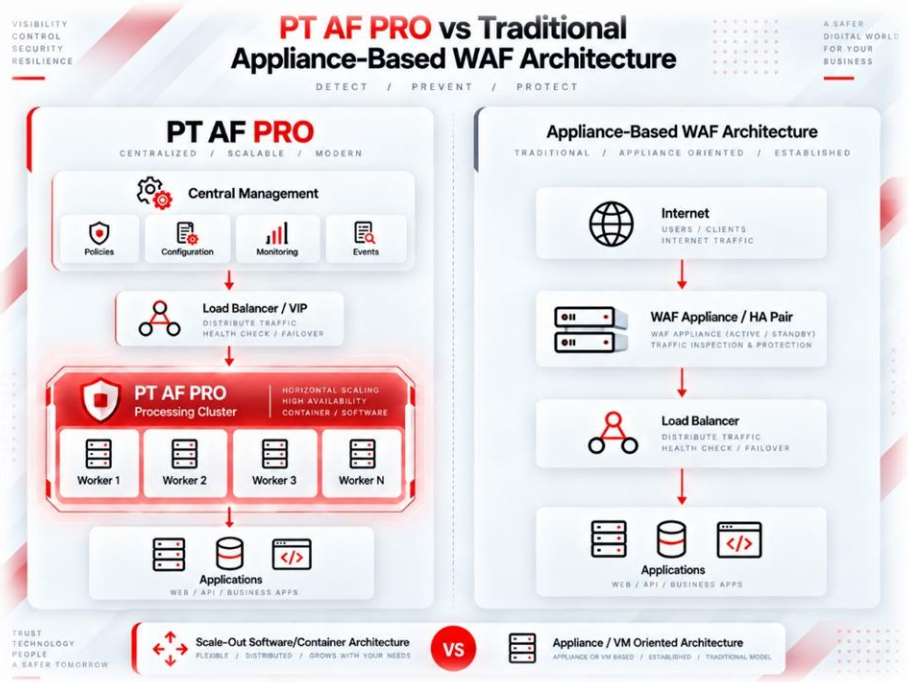
- Architecture
- Scalability
- Application Profiling
- Machine Learning
- API Security
- Bot Protection
- Zero-Day Detection
- Client-Side Protection
- Virtual Patching
- High Availability
- Management
- Integration
- Deployment Flexibility
- Performance
- Operational Complexity

PT AF PRO و FortiWeb

FortiWeb یکی از Enterprise WAFهای شناخته‌شده Fortinet است که برای حفاظت از Web Application و API طراحی شده است , نسخه‌های فعلی FortiWeb علاوه بر Signature Detection از Machine Learning، Application Profiling، Bot Mitigation، API Protection، Client-Side Protection، Vulnerability Scanner و Integration با سایر محصولات Fortinet استفاده می‌کنند. Fortinet همچنین FortiWeb را در قالب Hardware Appliance، Virtual Machine و سرویس‌های Cloud ارائه می‌کند.

بنابراین از نظر دسته محصول، PT AF PRO و FortiWeb هر دو در حوزه Enterprise Web Application and API Protection قرار می‌گیرند، اما معماری و شیوه Scale کردن آنها کاملاً یکسان نیست ,یکی از نقاط تمرکز مهم PT AF PRO معماری Container-based، Multitenancy، Centralized Management و Scale-out Processing است.

در مقابل FortiWeb علاوه بر نسخه Virtual، خانواده گسترده‌ای از Hardware Appliancesها را ارائه می‌کند و در برخی مدل‌ها از Hardware Acceleration برای افزایش WAF Throughput و پردازش Encryption/Decryption استفاده می‌کند , این تفاوت معماری در پروژه‌هایی که رشد Traffic، محدودیت Hardware، توسعه تدریجی Capacity یا Distributed Deployment اهمیت دارد، باید به صورت دقیق بررسی شود.



[تصویر شماره ۱۲]

مقایسه اولیه قابلیت‌های امنیتی

از نظر Security Feature، دو محصول در بسیاری از حوزه‌ها قابلیت‌های مشابهی ارائه می‌کنند :

- هر دو محصول برای حفاظت از OWASP Top ۱۰ طراحی شده‌اند.
- هر دو از روش‌های مبتنی بر Signature و مدل‌های رفتاری استفاده می‌کنند.
- هر دو دارای قابلیت Machine Learning برای شناسایی Anomaly و حملات ناشناخته هستند.
- هر دو قابلیت مقابله با Bot دارند.
- هر دو از API Protection پشتیبانی می‌کنند.
- هر دو دارای مکانیزم‌هایی برای مقابله با DoS در سطح Application هستند.
- هر دو امکان Virtual Patching یا محافظت از Vulnerability تا زمان اصلاح Application را ارائه می‌کنند.

FortiWeb در نسخه‌های فعلی خود قابلیت‌هایی مانند ML-Based API Discovery، Schema Verification برای XML و JSON، Bot Mitigation مبتنی بر Machine Learning و Biometric Detection، Client-Side Protection، Built-in Vulnerability Scanner و Integration با FortiSandbox را ارائه می‌دهد.

در مقابل PT AF PRO علاوه بر Application Profiling و Machine Learning، قابلیت‌های اختصاصی مانند WAF.js برای Client-Side Protection، M-Scan برای تحلیل فایل و P-Code برای Virtual Patching مبتنی بر تحلیل Source Code را در اکوسیستم خود ارائه می‌کند.

positive technologies
BUILD A SAFER DIGITAL WORLD

PT AF PRO vs FortiWeb – Initial Technical Comparison
Application Protection for Modern Business

REAL THREATS. PRACTICAL PROTECTION

Capability	PT AF PRO (Positive Technologies)	FortiWeb (Fortinet)	Notes
OWASP Top 10 Protection	Yes	Yes	Both protect against OWASP Top 10 classes.
Signature Detection	Yes	Yes	Rule/signature-based attack detection in both.
Machine Learning	Yes	Yes	PT uses profiling/behavioral ML; FortiWeb uses AI/ML application modeling.
Application Profiling	Yes	Yes	Both model normal application behavior.
Zero-Day Detection	Yes	Yes	PT uses anomaly/profile analysis; FortiWeb uses ML/anomaly detection.
API Protection	Yes	Yes	Both protect web APIs.
API Discovery	Limited / version-dependent	Yes	FortiWeb explicitly provides ML-based automatic API discovery.
Bot Protection	Yes	Yes	Both support malicious bot detection and control.
L7 DDoS Protection	Yes	Yes	Both provide application-layer DoS/DDoS mitigation.
Client-Side Protection	WAF.js	Yes	PT WAF.js protects browser-side threats; FortiWeb has Client-Side Protection.
Virtual Patching	P-Code / Rules	Yes	PT P-Code can create virtual patches; FortiWeb supports vulnerability-scanner-driven virtual patching.
Vulnerability Integration	Yes	Yes	Both integrate vulnerability findings into protection workflows.
Malware / File Inspection	M-Scan	AV / Sandbox	PT M-Scan supports multi-engine scanning; FortiWeb supports AV and sandbox-based file inspection.
Reverse Proxy	Yes	Yes	Supported by both.
Transparent Deployment	Yes	Yes	PT transparent proxy; FortiWeb inline/true transparent modes.
Sniffer Mode	Yes	Yes	PT SPAN/sniffer; FortiWeb offline sniffing/protection.
High Availability	Yes	Yes	Both support clustered/high-availability deployment.
Horizontal Scaling	Cluster processing nodes	Active/Active HA cluster	Different scaling approaches.
Multitenancy	Yes	Administrative Domains	PT native multitenancy; FortiWeb provides Administrative Domains with RBAC.
Centralized Management	Yes	Yes	Both support centralized administration.
Hardware Appliance	Supported deployment option	Yes	FortiWeb has dedicated hardware appliances; PT can be deployed on suitable server hardware/platforms.
Virtual Deployment	Yes	Yes	Both support virtualized deployment.
Cloud Deployment	Yes / PT Cloud AF ecosystem	Yes	FortiWeb is available in cloud/SaaS/public cloud form factors.
REST API / Automation	Yes	Yes	Both support API-based management/automation.

FROM PROTECTION TO RESILIENCE
SECURE APPLICATIONS. ENABLE YOUR BUSINESS.

positive technologies | PEOPLE. TECHNOLOGIES. A SAFER TOMORROW.

[جدول شماره ۴]

تا این مرحله می‌توان PT Application Firewall PRO را یک WAF صرفاً مبتنی بر Signature در نظر نگرفت، بلکه باید آن را به عنوان یک Application Security Platform با معماری قابل توسعه بررسی کرد.

ترکیب Signature Detection، Application Profiling، Machine Learning، User Profiling، Correlation، Bot Protection، Client-Side Protection، Virtual Patching و معماری Scale-out باعث می‌شود محصول بتواند در سناریوهای Enterprise و محیط‌های دارای تعداد زیادی Web Application و API مورد استفاده قرار گیرد.

معماری Container-based، Multitenancy و Centralized Management نیز برای سازمان‌هایی که چندین Data Center، شرکت زیرمجموعه یا مجموعه بزرگی از Applicationها دارند اهمیت ویژه‌ای دارد. Positive Technologies در سال ۲۰۲۶ نیز اعلام کرده تمرکز اصلی توسعه WAF خود را بر PT Application Firewall PRO و PT Cloud Application Firewall قرار داده است.

مقایسه جامع قابلیت‌های PT AF PRO و FortiWeb

مقایسه Enterprise WAFها باید در چند سطح انجام شود و محدود کردن آن به Detection Rate یا Throughput تصویر کاملی ایجاد نمی‌کند , جدول زیر مجموعه قابلیت‌هایی را که در طراحی و انتخاب Enterprise WAF اهمیت دارند در کنار هم قرار می‌دهد.

Capability	PT AF PRO (Positive Technologies)	FortiWeb (Fortinet)
OWASP Top 10 Protection	پشتیبانی می‌شود	پشتیبانی می‌شود
Signature-Based Protection	پشتیبانی می‌شود	پشتیبانی می‌شود
Machine Learning	پشتیبانی می‌شود	پشتیبانی می‌شود
Application Profiling	پشتیبانی می‌شود	پشتیبانی می‌شود
User Behavioral Analysis	پشتیبانی می‌شود	پشتیبانی می‌شود
Zero-Day Detection	Behavioral / ML	Behavioral / ML
Correlation	پشتیبانی می‌شود	Threat Scoring / Correlation
API Protection	پشتیبانی می‌شود	پشتیبانی می‌شود
Automatic API Discovery	وابسته به قابلیت نسخه و سناریو	قابلیت مشخص FortiWeb
API Schema Validation	بررسی بر اساس Policy و قابلیت نسخه	XML / JSON / OpenAPI
Bot Protection	پشتیبانی می‌شود	پشتیبانی می‌شود
ML Bot Detection	پشتیبانی می‌شود	پشتیبانی می‌شود
L7 DDoS Protection	پشتیبانی می‌شود	پشتیبانی می‌شود
Client-Side Protection	WAF.js	Client-Side Protection
Virtual Patching	P-Code / Security Rules	Vulnerability Scanner / Scanner Integration
Source Code-Based Protection	P-Code	رویکرد متفاوت
Malware File Analysis	M-Scan	AV / Sandbox Integration
Multiple AV Engines	M-Scan Architecture	Fortinet Security Integration
Built-in Vulnerability Scanner	Integration / PT Ecosystem	موجود
Reverse Proxy	پشتیبانی می‌شود	پشتیبانی می‌شود
Transparent Mode	پشتیبانی می‌شود	پشتیبانی می‌شود
Sniffer / Offline Monitoring	پشتیبانی می‌شود	پشتیبانی می‌شود
Load Balancing	ملزم معماری Architecture	Built-in L7 Load Balancing
SSL Offloading	پشتیبانی	پشتیبانی
Active-Passive HA	Cluster Architecture	پشتیبانی
Active-Active	Scale-out Architecture	پشتیبانی
Horizontal Scaling	Cluster Cluster / Processing Nodes	HA Cluster / Multiple Nodes
Container-Oriented Architecture	یکی از عناصر اصلی معماری	معماری متفاوت
Multitenancy	پشتیبانی	Administrative Domains
Central Management	پشتیبانی	پشتیبانی
REST API	پشتیبانی	پشتیبانی
SIEM Integration	پشتیبانی	پشتیبانی
Hardware Appliance	قابل استقرار روی Platform مناسب	خانواده Appliance اختصاصی
Virtual Deployment	پشتیبانی	پشتیبانی
Cloud Deployment	پشتیبانی / PT Cloud AF	پشتیبانی
Application Delivery Features	تمرکز اصلی Security	ADC گسترده ADC Features
Caching / Compression	وابسته به معماری	پشتیبانی
Content Routing	وابسته به معماری	پشتیبانی
Fortinet Security Fabric	—	Integration Native
PT Security Ecosystem	Integration Native	—

[جدول شماره ۶]

FortiWeb علاوه بر قابلیت‌های WAF، مجموعه‌ای از Application Delivery Featureها مانند Server Load Balancing ،Layer۷ ،SSL Offloading ،URL Rewriting ،Content Routing ،Compression و Caching ارائه می‌دهد. این موارد در Datasheet فعلی FortiWeb نیز ذکر شده‌اند.

از این منظر FortiWeb در بسیاری از Deploymentها می‌تواند بخشی از وظایف Application Delivery را نیز به طور مستقیم انجام دهد.

PT AF PRO در مقابل بیشتر بر Application Security، Detection، Scalability و ادغام با اکوسیستم امنیتی Positive Technologies تمرکز دارد.

ملاحظات انتخاب محصول

در فرآیند انتخاب WAF برای یک سازمان، پیشنهاد می‌شود حداقل موارد زیر در Proof of Concept بررسی شوند:

- تعداد واقعی Request Per Second
- HTTPS Throughput
- TLS Transaction Rate
- Latency ایجادشده توسط WAF
- تعداد Applicationهای قابل محافظت
- API Traffic Volume
- اندازه Request و Response
- File Upload Traffic
- Bot Detection Accuracy
- False Positive Rate
- Zero-Day / Anomaly Detection
- Policy Learning Time
- High Availability
- Failover Time
- Scale-Out Behavior
- Logging Performance
- SIEM Integration
- Management Complexity
- License Model
- Hardware Dependency
- Growth Capacity

نتیجه‌گیری

افزایش وابستگی سازمان‌ها به Web Applicationها، APIها و Digital Serviceها باعث شده Application Layer به یکی از مهم‌ترین سطوح حمله در زیرساخت فناوری اطلاعات تبدیل شود , در چنین شرایطی WAF دیگر صرفاً یک Firewall برای شناسایی SQL Injection و XSS نیست.

نسل جدید Application Security Platformها باید بتوانند رفتار Application و User را تحلیل کنند، APIها را محافظت کنند، Automated Attackها و Botها را شناسایی کنند، Zero-Day Attackها را تا حد امکان بر اساس Anomaly و Behavioral Analysis تشخیص دهند و در عین حال قابلیت توسعه متناسب با رشد Traffic سازمان را داشته باشند.

PT Application Firewall PRO با ترکیب چندین Detection Mechanism و معماری قابل توسعه، تلاش می‌کند این نیازها را در یک Platform یکپارچه پوشش دهد.

Application Profiling، Machine Learning، User Profiling، Correlation، API Protection، Bot Protection، WAF.js، M-Scan، P-Code، Multitenancy و معماری Cluster از اجزایی هستند که جایگاه محصول را فراتر از یک Signature-Based WAF سنتی قرار می‌دهند ,در مقابل، مقایسه با محصولی مانند FortiWeb نشان می‌دهد بازار Enterprise WAF به سمت Platformهایی حرکت کرده است که مجموعه‌ای از Web Security، API Security، Bot Management، Machine Learning و Application Delivery را یکجا ارائه می‌کنند. FortiWeb در نسخه‌های فعلی خود قابلیت‌های پیشرفته‌ای مانند ML-Based API Discovery، Schema Protection، Sensitive Data Leakage Detection، Bot Deception، Biometric Bot Detection و Client-Side Protection ارائه می‌دهد.

بنابراین تصمیم نهایی برای انتخاب میان PT AF PRO، FortiWeb یا سایر Enterprise WAFها باید بر اساس Architecture Requirement، حجم Traffic، نیاز API Security، مدل Deployment، Integration، Hardware Strategy و نتایج واقعی Proof of Concept انجام شود. در محیط‌هایی که معماری قابل توسعه، Independence بیشتر از Appliance خاص، Multitenancy و Distributed Processing اهمیت بالایی دارد، معماری PT AF PRO ارزش بررسی ویژه‌ای دارد.

در مقابل در محیط‌هایی که از اکوسیستم Fortinet استفاده می‌کنند یا قابلیت‌های Integrated Application Delivery، API Discovery پیشرفته و Appliance-Based Deployment بخشی از Requirement اصلی هستند، FortiWeb مجموعه فنی گسترده‌ای در اختیار طراح شبکه قرار می‌دهد , در نهایت، انتخاب WAF باید نه بر اساس یک Feature List تبلیغاتی، بلکه بر مبنای معماری واقعی سازمان، Traffic Pattern، Security Requirement، ظرفیت توسعه آینده و نتایج آزمون عملی محصول انجام شود.