HIGHLIGHTS

PT Application Firewall™ is a serious response to the challenges of protecting modern web portals, ERP systems, and mobile applications. It blocks 30% more network attacks than other firewalls due to its innovative security features:

- **Rapid adaptation to your system.** PT AF™ analyzes network traffic and system logs to create a real-time operational model of each application which is then used to detect abnormal behavior. Together with other protection mechanisms, it blocks 80% of zero-day attacks without requiring any special adjustment.
- **Focus on major threats.** PT AF™ weeds out attack attempts that do not represent a threat, groups similar incidents together, and detects attack chains.
- **Instant protection.** The virtual patching technology within PT AF™ allows companies to protect their applications before vulnerabilities in the code are fixed. Its source code analyzer and exploit generation function (P-Code) help to automatically detect vulnerabilities and prepare virtual patches. These features also provide developers with accurate information about vulnerabilities, which reduces testing and remediation costs.
- **Protection against bypassing technics.** PT AF™ handles data with regard to a protected server technology stack, analyzes XML, JSON, and other formats typically found in modern portals and applications. This helps to protect apps from most types of firewall bypass methods (HPC, HPP, Verb Tampering, etc.).
- **Protection against DDoS attacks on the application level.** PT AF™ guards against automated attacks including password bruteforcing, fraud, botnets, DDoS attacks, and data leakage.

PT APPLICATION FIREWALL™ BASED ON CISCO UCS C- AND E-SERIES: EFFECTIVE PROTECTION OF APPLICATIONS

Every year, enterprises come to rely more and more heavily on the internet. They offer mobile services for clients and use portal ERP solutions such as SAP SRM to interact with suppliers. Media apps and e-government portals are becoming increasingly popular. Although they offer high performance and improved efficiency, such technologies also present new opportunities for attackers to target the organizations that use them. According to a 2015 study by Positive Research, 47% of corporate system breaches could be traced to exploitation of vulnerabilities in web applications.

PT Application Firewall™ (PT AF™) is designed to ensure the effective and secure operation of web applications. Special editions of PT AF™ have been developed to provide targeted protection for e-banking and ERP systems (including those based on SAP), telecoms web services, e-government and mass media applications. PT AF™ provides early detection of attacks on applications, proactively detects code vulnerabilities, and blocks related security threats while the software is being fixed.

One of the preferred options for deploying PT Application Firewall™ is installation on the Cisco Unified Computing System (UCS) platform. The technologies used in Cisco UCS allow organizations to optimize their IT infrastructure and reduce costs related to equipment purchase, deployment, and maintenance. Cisco servers are integrated into the UCS domain. Using Cisco UCS Manager and Cisco SingleConnect technologies alongside predetermined policies and templates greatly simplifies the process of hardware configuration.

ADDITIONAL FEATURES

- Protection against all common vulnerabilities recognized by OWASP and WASC, including SQLi, XSS, and XXE, as well as against HTTP Request Splitting, Clickjacking, and complicated client-side attacks (DOM-based XSS).
- Proactive defense of queries, data, and cookies allows blocking such attacks as CSRF, even if developers have overlooked security tools.
- Compliance with PCI DSS and other national, international, and corporate standards.
- Effective integration into corporate information security management systems: integration with antiviruses, DLP and DDoS prevention technologies, SIEM, and other products included in the PT AppSec ecosystem.
- Protection against bots, plus anti-fraud mechanisms including services that detect abnormal client behavior.
- Support for the Content Security Policy (CSP) standard to prevent Cross-Site Scripting (XSS), Clickjacking, and other code injection attacks.
- SSL traffic analysis as an additional protection service.

UCS AND PT AF™: SCALING BACK SECURITY COSTS

Positive Technologies and Cisco have worked together to develop a joint solution in which PT Application Firewall™ can be purchased pre-installed and pre-configured on a choice of Cisco UCS hardware.

A solution based on the Cisco UCS E-Series platform provides customers with a router and an application firewall in one device, reducing the overall cost of network and application security. This is an ideal choice for smaller local divisions of distributed organizations that require an affordable solution for network traffic security.

Alternatively, PT AF™ can be pre-installed on Cisco UCS C-Series products that are designed for use in data processing centers and for protection of heavy-load applications.

Both solutions are flexibly integrated into a Cisco-based network infrastructure, reducing equipment purchase and support costs.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com