MULTILAYER APPROACH TO ADDRESS COMPLEX WEB AND NETWORK THREATS

POWERFUL SOLUTION
FROM POSITIVE TECHNOLOGIES AND CHECK POINT

POSITIVE TECHNOLOGIES

COLLABORATIVE SOLUTIONS FROM CHECK POINT SOFTWARE TECHNOLOGIES AND POSITIVE TECHNOLOGIES DESIGNED FOR CORPORATE NETWORK PERIMETER PROTECTION AND APPLICATION-LEVEL ATTACK PREVENTION

POSITIVE TECHNOLOGIES APPLICTAION FIREWALL ™

PT Application Firewall™ is an adaptive application-level firewall dedicated to the detection and blocking of attacks on web portals, ERP applications, and e-banking systems. Collaborative efforts of the vulnerability scanner and the correlation mechanism allows the detection of all attack stages and counteracting emerging threats with the sufficient amount of security resources that otherwise would be spent on irrelevant hacking attempts.

PT AF™ KEY ADVANTAGES:

- Adaptation based on the machine self-learning mechanism
- Intellectual analysis for abnormal requests and behavior detection
- Threat prioritizing and incidents linking, monitoring of attacks development
- Automated generation of virtual patches
- Behavioral analysis against bots

CHECK POINT SOFTWARE TECHNOLOGIES

- Next-generation security for your data center, enterprise, and small business
- Multilayer protection from known threats and zero-day attacks
- Open APIs leverage Positive Technologies web application security

Check Point®
SOFTWARE TECHNOLOGIES LTD.

The web applications industry has experienced unprecedented growth, especially in online banking systems, digital trading platforms, state services portals, and business apps. Companies are actively implementing online technologies and deploying complex security systems to protect those online technologies. However, unless these measures include a web application firewall, they will not be enough to protect against data leakage and unauthorized penetration inside corporate data systems, both of which are possible due to the existence of web application vulnerabilities. The statistics are alarming as, according to the Ponemon Institute polls, web services are the entry point for attacks on corporate networks in 78% of cases. Similar research, done by Positive Technologies, shows that 70% of web apps contain critical vulnerabilities.

Positive Research states that those attacks were mostly based on vulnerabilities found in web applications, so traditional infosecurity systems are ineffective. Therefore, it is now necessary to employ additional tools for web services protection in the form of web application firewalls. However, all the signature analysis mechanisms and heuristic algorithms for vulnerability detection that are utilized in application-level firewalls require a complex configuration process and may still be insufficient. That is why machine learning technologies that adapt themselves to the business logic of particular web applications and, combined with other Information Security instruments, allow timely blocking of malicious requests, application-level DoS, and detecting 0-day vulnerabilities are at the heart of Positive Technologies solutions.

Experts from Positive Technologies and Check Point Software Technologies consider security risks related to web technologies and internet access to be significant. So, the companies decided to come together and develop an integrated solution for a company's perimeter protection as well as its resources.

SECURITY STRATEGY

The implementation of this integrated approach to IS maintenance allows better protection of corporate systems and its associated data in the dynamically changing information environment. As a rule, this approach is realized in several stages that includes: activity analysis, abnormal behavior detection, alerts and source blocking. The approach works across all levels of a modern organization:

- User
- Application
- Data
- Infrastructure

Available software and hardware solutions allow building an efficient cybersecurity model for any organization.

CHECK POINT SOFTWARE TECHNOLOGIES AND PT APPLICATION FIREWALL™

Web application security is the most up-to-date trend supported by real cases of data leakage, online fraud, DoS attacks and other malicious actions that can cause reputational loss to a company.

Combination of the Check Point Software Technologies experience in network security and Positive Technologies vulnerability detection and elimination technologies provide maximum support for important web services and applications.

The approach ensures better protection of corporate systems and its associated data in the dynamically changing information environment and works across all levels of a modern organization: user, data, web applications, infrastructure.

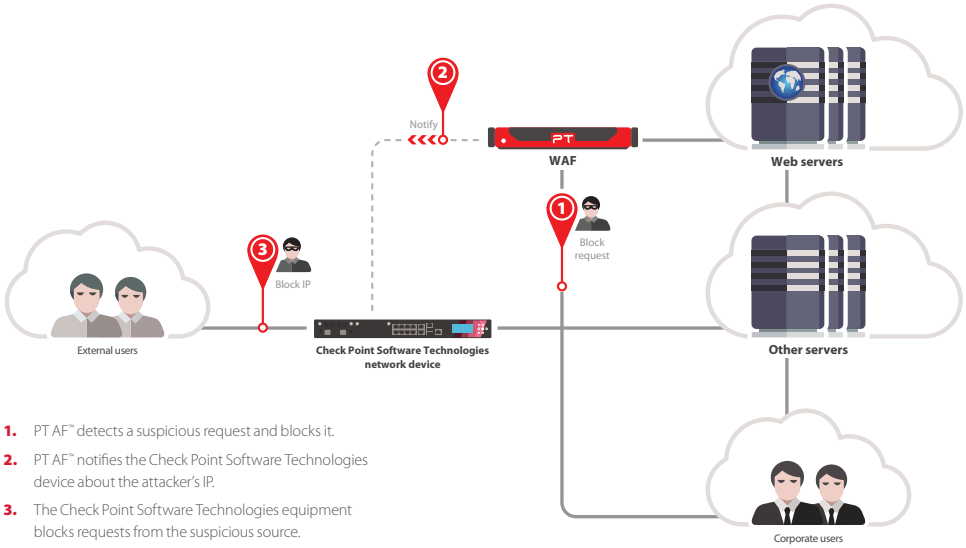
PROTECTION TECHNIQUES

Web App Protection in the Reverse Proxy Server Mode

The Check Point Software Technologies equipment protects the network perimeter and translates requests to web applications onto PT AF™.

PT AF™ is used for web application protection and operates in the reverse proxy server mode.

When detecting an attack, PT AF™ notifies the Check Point Software Technologies network device about the source's IP address and block timeout. The latter blocks further requests from the suspicious address on a network level.



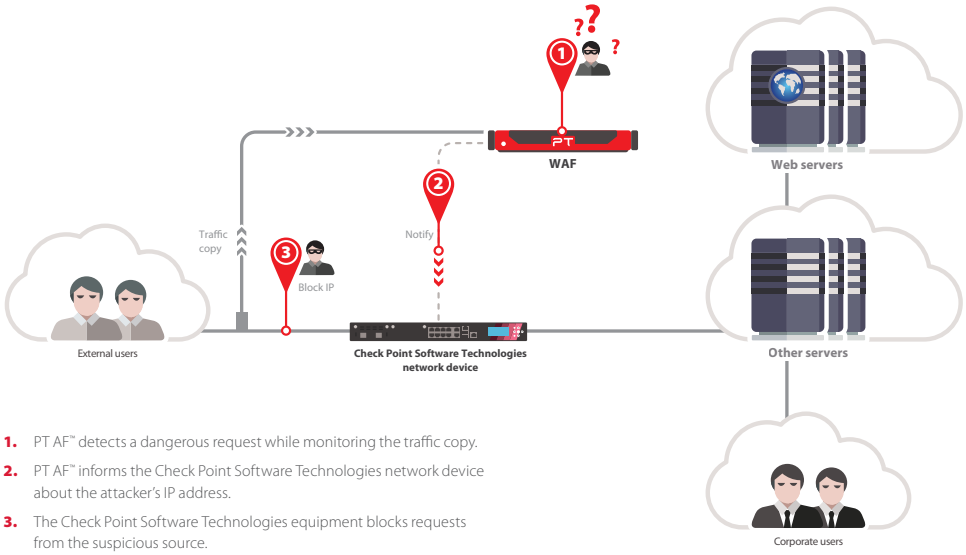
1. PT AF™ detects a suspicious request and blocks it.
2. PT AF™ notifies the Check Point Software Technologies device about the attacker's IP.
3. The Check Point Software Technologies equipment blocks requests from the suspicious source.

Stand-by Web Service Protection

External channels are terminated at a switch, network packet broker, or a test access point. The goal is to transfer a traffic copy of a web application to PT AF™.

The Check Point Software Technologies equipment protects the network perimeter. PT AF™ is used for web application protection and operates in a sniffer mode for traffic copy analysis.

When detecting an attack, PT AF™ notifies the Check Point Software Technologies network device about the source's IP address and block timeout. The latter blocks further requests from a suspicious address on a network level.



1. PT AF™ detects a dangerous request while monitoring the traffic copy.
2. PT AF™ informs the Check Point Software Technologies network device about the attacker's IP address.
3. The Check Point Software Technologies equipment blocks requests from the suspicious source.

THE ADVANTAGES OF THE SOLUTION

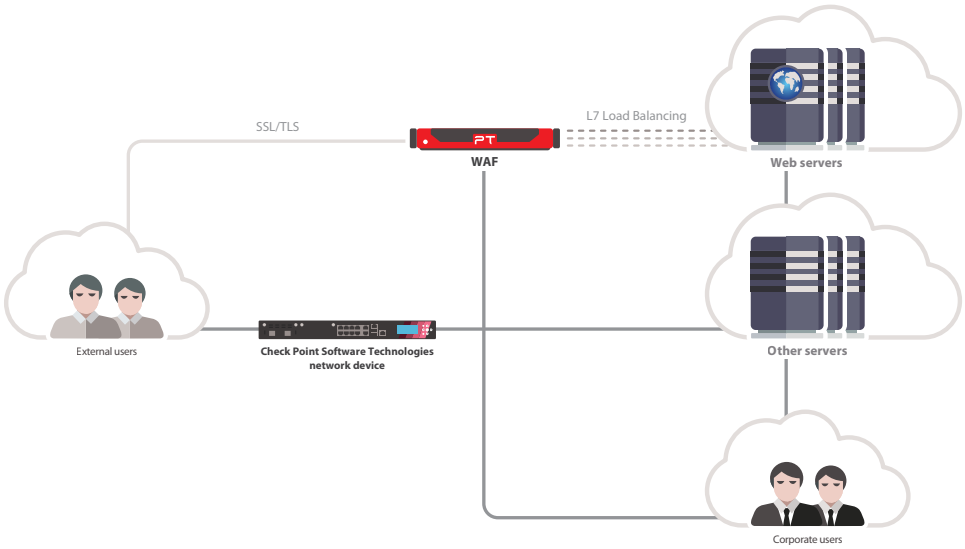
- Real-time protection of the perimeter and web applications
- Automated notifications about incidents for all operating Check Point Software Technologies network devices
- Protection against 0-day attacks thanks to machine self-learning mechanisms
- Protection against DoS attacks on applications and anomaly detection
- Multiple scaling options
- Extended functions for investigating IS incidents

SSL Traffic Protection

The Check Point Software Technologies equipment protects the network perimeter and translates requests to web applications. Web applications are protected using TLS/SSL protocols.

PT AF™ is used for web application protection and works in the reverse proxy server mode. It can decrypt traffic and protect web applications in accordance with security policies.

Understanding the context of web app operation helps PT AF™ provide efficient protection as well as to distribute requests among server groups, which ensures service accessibility.



Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest network cybersecurity vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises—from networks to mobile devices—in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

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