Fortinet’s New High-Performance Web Application Firewalls and Security Services Further Protect Customer Data from Attack and Data Loss

Enhanced FortiWeb Line Provides Higher Through put, Real-Time Security Updates, Sandbox Integration and Third-Party Web Application Vulnerability Scanning to Better Protect Web-based Applications and Internet Facing Data from Cyber Threats

Fortinet®, the global leader in high-performance cybersecurity solutions, recently announced the launch of its new FortiWeb 4000E and 3000E Web Application Firewalls (WAFs), designed to help customers prevent identity theft, financial fraud and denial of service through specialized, layered application threat protection. FortiWeb appliances now offer advanced security services backed by FortiGuard Labs’ advanced threat intelligence, providing real-time threat protection at the application level. These new FortiWeb solutions are also integrated with Fortinet’s FortiSandbox and offer support for new enhancements in partnership with Acunetix’s advanced vulnerability scanning solutions. These new additions bolster Fortinet’s broad end-to-end cybersecurity platform that protects customer data at every possible entry point to the network.

High-Performance Meets Advanced Layered Protection

The new FortiWeb 4000E delivers an unprecedented 20 Gbps WAF through put and features built-in advanced anti-malware capabilities – a first for the WAF appliance market – while also integrating leading vulnerability scanning features from Acunetix. Fortinet’s FortiWeb appliances provide the performance, effectiveness and features that only Fortinet can deliver, surpassing all competitive solutions and resetting expectations for web application firewalls.

The FortiWeb series of WAFs are now fully integrated with Fortinet’s FortiSandbox and Advanced Threat Protection (ATP framework), ensuring that organizations can arm themselves with seamless, end-to-end protection from even the most sophisticated cyber threats. These enhancements to FortiWeb deliver advanced, layered application threat protection for medium and large enterprises, application service providers and SaaS providers demanding the very best WAFs in the industry.

FortiWeb appliances can now receive real-time security updates from FortiGuard Labs, Fortinet's ground-breaking threat intelligence and research team. These consist of three services that can be delivered individually or in a bundle:
[if !supportLists]1. [endif]FortiWeb Security Service offers advanced and constantly updated defences against web vulnerabilities and suspicious URLs while also delivering application layer security.
[if !supportLists]2. [endif]The IP Reputation Service delivers advanced protection from botnet attacks.
[if !supportLists]3. [endif]Anti-malware and Anti-intrusion Services proactively protect against malware infections.

All of these services are delivered in real-time and sourced from Fortinet's global network of over 2 million security appliances. These sensors give Fortinet's FortiGuard Labs the widest visibility into new and existing threats and ensure that FortiWeb appliances are armed with the best possible application protection in the industry.

"Application Security is an increasingly important tool in the fight against Advanced Threats. However, with many of the Web Application Firewalls on the market today, customers have to trade off Performance for Security. This problem will only get worse as customers' network reliance and Data Center bandwidth requirements continue to increase," said John Maddison, vice president of marketing at Fortinet. "Fortinet is well known for the best combination of performance and security, with its Network Security products, and is now bringing that knowledge to bear for the benefit of customers with its FortWeb Application Firewalls."

"By virtue of continuously scanning evolving web apps and web sites with Acunetix Web Vulnerability Scanner, Fortinet users can now be assured that their web site security is being kept up to date regardless of what vulnerabilities could creep into their web site code through business pressures and forced short cuts in the development process. While not eliminating the need to promptly fix these issues, this will help reduce the pressure on security and dev teams. A warning though. Users should scan their web apps or web sites regularly to identify new vulnerabilities as they emerge," announced Chris Martin, GM, Acunetix.