TeamF1 Unveils Enhanced UTM Features for Security Gateways

FREMONT, Calif., June 1, 2011 (SEND2PRESS NEWSWIRE) — TeamF1, Inc. (www.TeamF1.com), the leader in embedded networking and security software solutions for wired and wireless applications, today announced availability of several new threat management features in its SecureF1rst platform in its highly-regarded Security Gateway Solution (SGS) for SMB security routers. The expanded set of features now enables OEMs to provide small and medium businesses with robust and ironclad protection from multiple types of threats including protection from viruses, malware, malicious web content, and poisoned URLs as well as offer them new VPN options and intrusion prevention features at layer 2 for WLANs.

This enhanced SecureF1rst SGS offering expands on its existing perimeter security features of firewall, IPS, and gateway anti-virus checks, to add new AV signature providers and zero-hour protection of businesses from the latest outbreaks of malware on the web aided by a continuously updated cloud-based filtering database.

TeamF1's InstanTunnel VPN security suite which includes IPsec, clientless SSL and PPTP VPN options, now offers an additional OmniSSL feature which offers site-to-site SSL VPN tunnels, interoperability with widely available OpenVPN™ servers and clients, as well as a unique mechanism to enable secure access to the LAN behind the router via a "cloud-gateway," from a user account on OpenVPN's commercial Access Server.

On the WLAN security side, new wireless intrusion prevention (WIPS) features in the SecureF1rst platform offer the ability to monitor Wi-Fi® traffic for guarding against threats from rogue access points, and protecting businesses by thwarting several common attacks such as "evil twin" and "man-in-the-middle" attacks.

"The landscape of network-based threats is continually evolving and gateway security solutions have to keep up with new levels of sophistication in security attacks," said Rohit Sukhija, Director of Marketing at TeamF1, Inc. "SMB network users and IT administrators demand comprehensive threat management features traditionally the domain of high-end enterprise equipment. By making new innovative security features available in a pre-integrated solution at an attractive price point, TeamF1 helps SMB networking OEMs rise to the challenge and deliver such devices to the market speedily."

The new features are available for immediate licensing on SecureF1rst SGS directly from TeamF1, and will also be rolled out to other turnkey solutions in TeamF1's SecureF1rst family in coming months.

About TeamF1:
TeamF1, Inc. a privately held corporation headquartered in Fremont, California, is a leader in high performance embedded networking and security

software. TeamF1's products enable secure networking of telecom/datacom and industrial equipment. For more information visit http://www.TeamF1.com or contact TeamF1 Public Relations at 510-505-9931.

Names mentioned are trademarks, registered trademarks or service marks of their respective companies.

News issued by: TeamF1, Inc.

Original Image: https://send2pressnewswire.com/image/11-0530-secure1st_72dpi.jpg

# # #

Original Story ID: 2011-06-0601-005 (7006) :: 2011-06-0601-005-Unified-Threat-Management

Original Keywords: Unified Threat Management, UTM, WLAN security options, OEM SMB gateway device software, SecureF1rst SGS, TeamF1, OmniSSL feature, openvpn, wi-fi, wireless intrusion prevention, Rohit Sukhija, cloud-based filtering database TeamF1, Inc. Fremont California FREMONT, Calif.

Alternate Headline: TeamF1, Inc. Unveils Enhanced Unified Threat Management Features for Security Gateways