FEDERATED
NETWORKS
connect secure

OWASP Top 10 Web Application Threats Eliminated by FN Connect Secure Web Application Gateway, BT Ethical Hacking Center Testing Shows

FOR IMMEDIATE RELEASE

Second in a Series of Independent Tests Demonstrates Effectiveness of Federated Networks' Breakthrough Cyber Security Technology

TORONTO, Ontario Ontario—December 8, 2010—**Federated Networks** today announced the results of the second in a series of independent tests by the BT Ethical Hacking Center. The tests demonstrate that the **FN Connect Secure Architecture** is able to prevent certain attacks that capitalize on common security vulnerabilities inherent in web applications. When the FN Connect Secure Web Application Gateway is deployed using Federated Networks Application Security Layer (ASL) protocol, BT Ethical Hacking Center testers were unable to capitalize on any of the 2010 top 10 web-based vulnerabilities, as outlined by the Open Web Application Security Project (OWASP). Additionally, BT testers were unable to penetrate a web server admin console's login, even when provided with the correct username and password to the application. An earlier tes by BT proved the efficacy of the **FN ASL protocol**, which thwarts common network vulnerabilities, such as phishing and man-in-the-middle attacks.

OWASP has long noted the vulnerable nature of many websites and posts a regular list of the top 10 web-based vulnerabilities, including SQL Injection and Cross-Site Scripting (XSS) that have historically been used by hackers to steal valuable data. To validate the effectiveness of its solution, Federated Networks and BT devised an innovative validation approach that leverages the OWASP 2010 top 10 and its related software security training website, Webgoat, which is a deliberately insecure web application designed to teach web application security lessons.

"Our basic premise was to take a well-known insecure application, like Webgoat, and see if we could fully secure it simply by adding the FN Connect Secure Web Application Gateway and running the FN ASL protocol," said David Lowenstein, Chief Executive Officer of Federated Networks. Given the growing use of cloud services, the need for secure cloud login has become an imperative and we are very pleased that the BT Web Admin Login tests confirmed that any FN protected web authentication can be made secure even if an attacker knows the username and password – in other words, FN's solution can even thwart the dreaded sticky tab attack. Simply put, our results, validated by BT's Ethical Hacking Center, show that by simply deploying FN, an enterprise or any developer of a web application can ensure the security of user data and deploy the solution in minutes and with costs starting at only a couple of hundred dollars per server."

Historically, various approaches such as code review, mathematical proofs and more recently application firewalls have been utilized with varying degrees of success in an effort to eradicate web application vulnerabilities. In all cases however, current solutions have thus far proven ineffective in stymieing pervasive code-related vulnerabilities. In addition, their implementation requires material cost in terms of organizational time, money and/or human resources.

"The bottom line is that coding is a human process and humans make mistakes, which are very difficult to consistently and completely identify and rectify in software code bases that are constantly being modified," said Risu Na, Chief Technology Officer of Federated Networks. "So we have built in a layer of redundancy that effectively immunizes web application code from being exploited. Simply put, Federated Networks has

Contact

David Lowenstein
CEO, Federated Networks
T: 905-361-2834
Dave@FederatedNetworks.com

Shweta Agarwal
Schwartz Communications
781-684-0770
federatednetworks@schwartz-pr.com

FEDERATED
NETWORKS
connect secure

added a new layer, namely 'neutralize,' to the existing layered software security model of 'Prevent, Detect, Monitor and Recover,' whereby Federated Networks' Connect Secure Architecture components effectively immunize users from broad classes of known attack vectors, thus neutralizing the effects of hacker attacks on systems and data."

Reports on both BT tests are available on the Federated Networks' **website**, along with more technical information about the company's products and technology. The results of a third test by BT, which will evaluate the FN Connect Secure Client/Agent, is expected to be released in the coming weeks.

The FN Connect Securely™ Framework provides the foundational infrastructure for securing planned Internet initiatives, such as secure e-statements and e-billing, e-voting, e-currency and e-health applications. Additionally, the company's technologies significantly strengthen military mission critical command and control IT infrastructure including solving several of the U.S. military's most challenging cyber security challenges, as outlined by the INFOSEC Research Council's "Hard Problems List." The company plans to provide additional details and demonstrations of these future friendly initiatives in the coming weeks.

About Federated Networks

Federated Networks enables consumers, corporations and government to Connect Securely™ to all things digital. Leveraging its 100 percent military-grade managed code base, the FN Connect Securely™ Architecture seamlessly and comprehensively protects content and communications against networked software's most pervasive threat vectors. Federated Networks' breakthrough cloud native, zero-knowledge protocol defends against identity theft and data compromise of any kind, whether it resides on social networks or secure servers. Ushering in a new era of cyber confidence, Federated Networks enables user centric control of the security and access rights of personal information and data. Founded in 2005, Federated Networks is privately held and headquartered in Toronto, Ontario. For more information please visit **http:// www.federatednetworks.com.**

About BT Managed Security Solutions Group

As the authority on enterprise security, BT's Managed Security Solutions Group combines managed security services portfolio with an Ethical Hacking Center of Excellence, offering its customers one of the only true end-to-end security solutions in the industry. BT has been offering security services to the fortune 1000 since 1991 and has performed thousands of Ethical Hacking assignments on a variety of systems and applications, including network infrastructure, online banking and trading and ecommerce. BT's Ethical Hacking (EH) services enable customers to protect their networks, information assets, and corporate reputations by identifying vulnerabilities before they can be exploited.

FEDERATED NETWORKS
2425 Matheson Boulevard, 7th Floor, Mississauga, Ontario L4W 5K4, Canada P. 905-361-2834 F. 416-622-3651
info@federatednetworks.com www.federatednetworks.com