FEDERATED
NETWORKS
connect secure

BT Ethical Hacking Center Validates Significant Security Advances of Federated Networks' ASL Protocol

FOR IMMEDIATE RELEASE

Independent Vulnerability Assessment Validates How Federated Networks' Breakthrough Cyber Security Solutions Fix Fundamental Flaws with SSL

TORONTO, Ontario November 18, 2010—**Federated Networks** today announced the BT Ethical Hacking Center recently confirmed that Federated Networks' ASL protocol **eliminates pervasive vulnerabilities** inherent in the known limitations and weaknesses of current SSL implementations. In independent testing, Federated Networks' new ASL protocol thwarted serious network-centric security attacks such as phishing, pharming, DNS Poisoning, and proxying, or more generally all forms of man-in-the-middle (M-I-M) attacks.

The testing is the first in a series of ethical hacking vulnerability assessments to be performed by BT to evaluate Federated Networks' **FN Connect Secure Architecture**, which comprehensively secures consumers, enterprises and governments wishing to protect their private and confidential data from networked software's most pervasive threat vectors.

"We are very pleased to have an ethical hacking firm of the caliber and pedigree of BT to validate the threat mitigation properties of the products, solutions and security technologies that are part of the FN Connect Secure Architecture," said David Lowenstein, chief executive officer of Federated Networks. "The bottom line is that security products should secure while also being secure, and these validations are an important first step in corroborating the efficacy of our solutions."

"Federated Networks' protocol is proven to be materially more secure than the existing SSL implementations that the rest of the industry and all of our competitors rely on," said Risu Na, chief technology officer of Federated Networks. "The fact that a plethora of here-to-fore troubling network threats such as phishing and more generally all forms of M-I-M attacks can now be provably 'neutralized' is an important development that we believe materially alters the terrain of the threat landscape."

BT's tests confirm that online security is indeed possible by eliminating the root issues inherent in other security approaches, as demonstrated by the FN Connect Secure Architecture's elimination of certain aspects of network security vulnerabilities. Simply put, FN has added a new layer, namely "Neutralize," to the existing layered software security model of "Prevent, Detect, Monitor and Recover," whereby FN's Connect Secure Architecture components effectively immunize users from broad classes of known attack vectors, thus "Neutralizing" hacker attacks on systems and data.

Federated Networks has made available on its website a more detailed report of BT's findings related to the efficacy of the FN ASL protocol and its ability to thwart common network vulnerabilities. Also available on the company's website is more technical information about the company's **products, solutions** and **technology.** The second and third elements of BT's testing related to the FN Connect Secure Architecture, namely the vulnerability testing of the FN Connect Secure Client and Agent, are expected to be finalized in the next 30 days. Importantly, the FN Connect Securely™ Framework provides the foundational infrastructure for securing

Contact

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

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

FEDERATED
NETWORKS
connect secure

planned Internet initiatives, such as secure e-statements and e-billing, e-voting, e-currency and e-health applications. Furthermore, 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 months.

About Federated Networks

Federated Networks enables consumers, corporations and government to Connect SecurelyTM to all things digital. Leveraging its 100 percent military-grade managed code base, the FN Connect SecurelyTM 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