

CONTACTS:

Joanne Heslop / Nick Daines
Insight
01625 500800
jheslop@insightmkt.com

Angela Hesse
Cisco Systems (UK)
0208 824 4478
ahesse@cisco.com

Cisco Extends and Enhances SAFE Security Blueprint With Introduction of New Firewall and Intrusion Detection Solutions

SAN JOSE, Calif., September 4, 2001 - Continuing to expand its technical and market leadership by delivering practical security and VPN innovations for real-world business demands, Cisco Systems, Inc. today announced a series of rich solutions to enhance and extend its SAFE security blueprint. These include the introduction of the Cisco PIX® 501 Firewall for small office/home office environments, and the Cisco IDS Host Sensor, a new host-based intrusion detection solution protecting critical server resources.

The SAFE blueprint is a flexible, dynamic blueprint for security and VPN networks, based on Cisco AVVID - the Architecture for Voice, Video and Integrated Data - that enables businesses to securely and successfully take advantage of e-Business and compete in the Internet economy. More information is available at <http://www.cisco.com/go/safe>

"SAFE provides defense-in-depth and strong data privacy for organisations of all sizes by recommending ways to implement scalable, cost-effective, best-in-breed security solutions throughout the e-Business infrastructure," said Richard Palmer, vice president and general manager of the Cisco VPN and Security Services business unit. "Today's announcement further extends our strategy of delivering complete solutions for fortifying all of the critical components in a network."

The new solutions and enhancements address many of the critical components of a secure network, including perimeter security, intrusion protection, management, and secure connectivity.

Specific elements of today's announcement include:

- **Perimeter Security:** The Cisco PIX 501 Firewall (see separate release issued today), a new security appliance for small office/home office environments which packs all the power, flexibility and functionality that customers have come to expect from high-end

PIX Firewalls in a compact, cost-effective, plug-n-play device. Ideal for "always-on" broadband connections, the PIX 501 includes stateful inspection firewalling, VPN and intrusion detection capabilities as well as an integrated 4-port 10/100 Mbps switch for small office or home office networking.

- **Intrusion Protection:** The Cisco IDS Host Sensor (see separate release issued today), is a software solution that proactively detects malicious activity and blocks access to server resources before damage can occur. Cisco today also announced significant extensions to its network-based IDS solutions, including the release of version 3.0 of its market-leading network-based IDS appliance software, Cisco IDS Network Sensor.
- **Management:** The CiscoWorks VPN/Security Management Solution (VMS) has added IDS Host management, giving it management support for both Cisco's network-based and host IDS solutions. Also available is a new version of Cisco Secure Policy Manager, including new task-based, easy-to-use GUIs and wizards. The VMS suite of products provides one-stop shopping for VPN and Security management.
- **Secure Connectivity:** The VPN Acceleration Module (VAM), an add-on blade for Cisco 7100 and 7200 Series routers, delivers high-performance IPSec encryption throughput for head-end site-to-site VPN deployments, providing customers a 60% increase in VPN scalability. The combination of rich IOS features-including support for routing, Quality of Service (QoS), multicast, and multi-protocol traffic across the VPN-and the VAM's high-performance hardware-assisted encryption sets the Cisco 7200 and 7100 series apart in site-to-site VPN solutions. (For more details please visit http://newsroom.cisco.com/dlls/prod_090401d.html)

Cisco is also introducing the VPN Client v3.1, the latest version of Cisco's award-winning client software providing enhanced software update notification capabilities, access to local network resources while tunneling other data and support for third party personal firewall software within the Cisco Unified Client Framework. These new enhancements offer a superior set of new features for remote access deployments. Additionally this latest release includes new public key infrastructure (PKI) authentication support from Entrust, offering customers a more scalable and manageable authentication solution for remote access VPNs.

Also available is Version 3.1 of the Cisco VPN 3002 Hardware Client, including added PPPoE support, eliminating the need for additional software or hardware to connect to PPPoE based DSL connections.

"The key value that Cisco provides its customers is that, because of its heritage in the enterprise and its comprehensive portfolio of security solutions, they're helping integrate security where the internal network touches the public Internet," said Joel Conover, senior analyst, Current Analysis.

"With SAFE, Cisco is helping its customers to be more secure and effective with a comprehensive approach to laying out all of their network security components."

Cisco Network Security Solutions

Indeed, complementing the SAFE security blueprint, Cisco offers a comprehensive array of market-leading, enterprise network security solutions to make implementation and maintenance of good network security easier and more cost-effective. These solutions encompass the key elements of network security and include dedicated appliances, software, consulting services, and security capabilities embedded into other Cisco network infrastructure products. In addition, Cisco works with an elite group of third-party vendors as part of the Cisco AVVID Partner Program that provide complementary products and services in order to meet the unique demands of enterprise customers. More information is available at <http://www.cisco.com/go/security>

About Cisco Systems

Cisco Systems (NASDAQ: CSCO) is the worldwide leader in networking for the Internet. Cisco news and information are available at <http://www.cisco.com>.

###

Cisco, Cisco Systems, PIX, IOS and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0005R)

http://newsroom.cisco.com/dlls/prod_090401.html

http://newsroom.cisco.com/dlls/prod_090401b.html

http://newsroom.cisco.com/dlls/prod_090401c.html

http://newsroom.cisco.com/dlls/prod_090401d.html

http://newsroom.cisco.com/ts_images/IDShost.jpg

http://newsroom.cisco.com/ts_images/VAM2.jpg

http://newsroom.cisco.com/ts_images/VAM.jpg

<http://www.cisco.com/warp/public/779/largeent/issues/security/safe.html>