FOR IMMEDIATE RELEASE

Press Contacts:

Perveen Akhtar   Debbie Leah
Cisco Systems   Insight Marketing & Communications
+44 (0) 020 8824 4478   +44 (0) 1625 500800
pakhtar@cisco.com   dleah@insightmkt.com

Cisco Teams with Network Associates, Symantec, and Trend Micro to Address Critical Industry Security Issues

Cisco Network Admission Control Increases Networks' Ability

to Defend Against Security Threats

LONDON, UK November 18, 2003 –Cisco Systems, Inc., today announced the Cisco® Network Admission Control program to address the increased threat and impact of worms and viruses to networked businesses. This strategic program represents a significant step forward in industry collaboration and is part of Cisco's Self-Defending Network Initiative that helps customers identify, prevent and adapt to security threats.

"As the network continues to be a mission critical business system for organizations of all sizes, a top priority for customers is securing their information assets and minimizing the impact of viruses and worms," said John Chambers, president and CEO of Cisco Systems, Inc. "Cisco's Network Admission Control program is designed to address a pervasive customer concern by helping organizations contain security threats before they cause damage

The Cisco Network Admission Control program was developed in conjunction with leading anti-virus software vendors including Network Associates, Symantec, and Trend Micro. This collaboration addresses the broad and growing concern among enterprise customers – the remediation costs resulting from worms and viruses.

"Recent worm and virus infections have elevated the issue of keeping insecure nodes from infecting the network and have made this a top priority for enterprises today," said Mark Bouchard, senior program director, META Group. "Many organizations were successful at stopping recent worm attacks at their Internet boundaries, yet still fell victim to the exploits when mobile or guest users connected their infected PCs directly to internal local area networks. Eliminating this type of threat will require a combination of strengthened policies and network admission control systems."

Customers using network admission control systems can allow network access only to compliant and trusted endpoint devices (for example, PCs, servers, personal digital assistants) and can restrict the access of non-compliant devices. In its initial phase, the Cisco Network

Admission Control functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This decision can be based on information about the endpoint device such as its current anti-virus state and operating system patch level. Network admission control systems allow non-compliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources. Cisco Network Admission Control systems will initially support endpoints running Microsoft Windows NT, XP and 2000 operating systems.

"The proliferation of unknown computing endpoints in the form of remote and mobile users puts our strategic information assets at increasing risk," said Lance Braunstein, chief information security officer, and executive director of Infrastructure Engineering, Morgan Stanley Individual Investor Group, a global financial services firm. "Cisco's collaboration with anti-virus software vendors will enable us to apply a consistent security policy to computers that access our network. Network admission control systems will allow us to take advantage of our existing investment in security software and network infrastructure to ensure that computers accessing our network will conform to our security policies."

A key component of the Cisco Network Admission Control program is innovative software developed by Cisco called the Cisco Trust Agent which resides on an endpoint system and communicates with the Cisco network. The Cisco Trust Agent collects security state information from multiple security software clients, such as anti-virus clients, and communicates this information to the connected Cisco network where access control decisions are made and enforced. Cisco has licensed its Cisco Trust Agent technology to Network Associates, Symantec and Trend Micro so it can be integrated with their security software client products.

The Cisco Trust Agent will also be integrated with the Cisco Security Agent to enforce access privileges based on an endpoint's operating system patch level. The Cisco Security Agent is Cisco's laptop/desktop and server host intrusion prevention and distributed firewall software that identifies and prevents malicious behavior before it can occur.

Cisco Self-Defending Network Initiative

The Cisco Network Admission Control program is a key development in the Cisco Self-Defending Network Initiative, an innovative, multi-faceted security strategy designed to dramatically improve the ability of networks to identify, prevent and adapt to a range of security threats. The Cisco Self-Defending Network Initiative advances Cisco's strategy of integrating security services throughout Internet Protocol (IP) networks by delivering new system-level network threat defense.

Network Admission Control Availability

Cisco Network Admission Control functionality is scheduled to be supported on Cisco's access and mid-range routers in mid-2004. In future releases, this capability will be extended across multiple Cisco product platforms, including switches, wireless access points and security appliances. The Cisco Trust Agent is scheduled to be integrated with both Cisco and some Cisco Network Admission Control program supporting companies' security client software products beginning in mid-2004. Future phases of this program will extend endpoint and network security interoperation to include infection containment capabilities. Cisco expects to open elements of the Cisco Network Admission Control program to additional organizations in the industry as the program develops.

Note to Editors: For more information on this announcement, a live webcast will begin at 10:30 am PST on November 18th, 2003. Interested parties can register at: http://www.corporate-ir.net/ireye/ir_site.zhtml?ticker=28103&script=1010&item_id=808249

An audio only option will also be available at this time by dialing 1-888-810-9160. International callers can dial 210-234-0050. Passcode is NAC.

About Cisco Systems

Cisco Systems, Inc.(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, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.

###