



UK Press contacts:

Sam Burrough
Cisco Systems
+44 (0)20 8824 1000
sburroug@cisco.com

Toby Walsh / Simone Huber
Brands2Life
+44 20 7592 1200
cisco@brands2life.com

Cisco Expands its Network Admission Control Framework to Strengthen IT Security Compliance

VIENNA, Austria, Oct. 18, 2005– Cisco Systems®, Inc. today announced advancements to its Network Admission Control (NAC) framework that help protect organizations from threats such as spyware, viruses and worms attempting to gain network access through a growing number of endpoint devices.

The Cisco NAC framework now includes support for Cisco Catalyst switch and wireless solutions, the expansion of the NAC partner program to include a new agentless auditing category, and enhancements to the NAC appliance family (formerly known as the Cisco Clean Access family). Together these advancements expand upon the Cisco Self-Defending Network security strategy that helps customers better identify, prevent and adapt to an ever-changing landscape of security threats.

"Companies the world over are continually looking to help ensure they protect and have control over all devices gaining access to the company network, in compliance with ever tightening corporate security policies," said Chris Thatcher , North American principal consultant for security for Dimension Data, a global IT services and solutions provider. "The advancements to the NAC framework mean that organizations are now able to take more advantage of their network infrastructure, security and management software investments and help enable the assessment of the security state of wired and wireless clients. This allows organizations to help enforce security policy by either granting or denying access to network resources based on client compliance with security policy. This will help provide an even more secure network environment via this controlled access."

Cisco Introduces New NAC Framework Deployment Scenarios

In addition to wide area network (WAN) environments, customers now have tools to help identify non-compliant systems before they get access to LAN and wireless network environments, trigger and perform a security posture or "health" assessment, and quarantine non-compliant systems for remediation. This information is collected and shared between NAC

framework components through a new version of the Cisco Trust Agent (CTA) version 2.0, a key endpoint technology in the NAC framework. By extending the NAC framework to the Catalyst switching portfolio and wireless solutions, customers now have a new resource to block threats before they have a chance to enter the local area network (LAN) and potentially infect other enterprise resources.

Cisco is also introducing improved abilities to assess the security risk of unmanaged or agentless endpoints/devices, that do not support the CTA and are attempting to gain network access. This is accomplished through collaboration with a new auditing category of NAC partner program vendors. Vendors joining this new category include Altiris, Qualys, and Symantec (through the WholeSecurity acquisition). Collaboration with these vendor solutions helps the NAC framework dramatically improve its ability to assess the risk of agentless devices such as guest laptops, printers, PDAs, and Internet Protocol telephones. These devices can now be audited by this new category of partners. The audit results will then be communicated back to the network to enforce the proper network admission decision.

These advancements, coupled with the integrated solutions offered by over 60 NAC vendor program participants in security and patch management software, extend customers' ability to utilize their existing infrastructure and software investment for an operationally efficient admission control system that helps reduce risk while ensuring higher network availability and increased business productivity.

Introducing Enhancements to Cisco NAC Appliance Family

Cisco is also announcing a new release of Cisco's family of turnkey NAC appliances, which can scan, block, quarantine and remediate non-compliant devices and enforce security policy. This new version offers a hardware appliance option in addition to the currently available software option for more deployment flexibility.

The NAC appliance family also comes with pre-configured anti-spyware checks from most major anti-spyware vendors. This provides customers with convenient and efficient management of anti-spyware software across a network protected by a NAC appliance as well as another layer of anti-spyware protection. This new version of the Cisco NAC appliance also includes single sign-on capabilities with both the Cisco ASA 5500 series and Cisco VPN 3000 series remote access concentrators which extends network admission control to remote access users without complicating the user experience.

For more information about the Cisco NAC framework and the Cisco products involved please visit: www.cisco.com/go/NAC

Pricing and availability

NAC framework support on the Cisco Catalyst 6500, 4500, 4900, 3700, 3500, and 2900 series switching platforms is scheduled to be available at the end of November 2005 as a part of a software upgrade and at no additional charge to customers with the corresponding product support contracts.

NAC framework support on the Cisco wireless platforms including Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), Cisco Aironet access points, Cisco Aironet lightweight access points and Cisco Wireless LAN Controller platforms are available today as part of Cisco IOS Software Release 1.4.1, Cisco IOS Software Release 12.3(7)JA or Cisco Unified Wireless Network Software Release 3.1 at no additional charge to customers with corresponding product support contracts.

The Cisco NAC appliance is offered as hardware bundle and as software only and is scheduled to be available at the end of November 2005 starting at \$8995 USD.

Other NAC framework components include:

- **Cisco Trust Agent version 2.0:** Scheduled to be available at end of November 2005 at no additional charge.
- **Cisco Access Control Server (ACS) version 4.0:** Scheduled to be available at end of November 2005 starting at \$7995 USD.
- **Cisco Secure Monitoring, Analysis, and Response System (CS-MARS) version 4.1:** Available today starting at \$15,000 USD.

About Cisco Systems

Cisco Systems, Inc. (NASDAQ: CSCO), the worldwide leader in networking for the Internet.. Information about Cisco can be found at <http://www.cisco.com>. For ongoing news, please go to <http://newsroom.cisco.com>

###