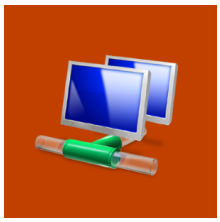
13 October 2008

By: Marius Oiaga, Technology News Editor



Windows Vista
Network
Microsoft

Network Access Protection for XP SP3 and Vista SP1

From Windows Server 2008 - design guide

Network Access Protection is designed to permit a high degree of control over client computers across a network. A critical feature of Windows Server 2008, NAP is now also supported by Windows Vista RTM and Service Pack 1 and Windows XP Service Pack 3. But deploying NAP is not exactly an effortless task. However, Microsoft is offering the necessary resources to help network administrators, infrastructure specialists and system architects. An illustrative example of this is the Network Access Protection Design Guide available via TechNet.

"The Network Access Protection Design Guide, authored by our very own technical writer and NAP Forum hero Greg Lindsay, is now live! The NAP Design Guide explains the advantages, disadvantages, requirements, recommendations, and design considerations for deploying NAP for the IPsec, 802.1X, VPN, and DHCP enforcement methods. (...) Huge thanks to Greg for his authoring efforts over the last year and to many NAP product team reviewers for helping to ensure that the content is technically accurate and complete," revealed Joe Davies, NAP Senior Program Manager.

The documentation covers a variety of aspects, with a strong focus on NAP with IPsec enforcement; NAP with 802.1X enforcement; NAP with VPN enforcement; NAP with DHCP enforcement; and NAP-NAC enforcement. The guide offers the necessary process for data gathering to permit the planning, designing and deployment of NAP.

In the end, the resource will allow for NAP to be tailored to a specific environment. Following deployment, client machines in an IT infrastructure will be able to access the network only in relation to the level in which they align with the overall governance policy. "If a client is not compliant, NAP provides a mechanism for automatically bringing the client into compliance (a process known as remediation) and then dynamically increasing its level of network access," Lindsay said.