Major Communications Infrastructure Provider Enhances Wireless Network with Windows XP and Windows Server 2003

Published: February 2003

Building on the success of its first phase of deployment of the Microsoft Windows XP Professional operating system, Enterasys Networks implemented a public key infrastructure to enable secure wireless access for employees, consultants, and contractors at offices worldwide and automatically enrolled all employees and their machines for certificates in just two days. Enterasys also is taking advantage of synergies between Microsoft Windows Server 2003 Enterprise Edition and Windows XP to implement more consistent configuration and lockdown practices for further enhancing the manageability and security of its environment.

Situation

In late 2001, Enterasys Networks completed a deployment of the Microsoft® Windows® XP Professional operating system to 2,000 desktop and portable PCs worldwide. This move enabled the worldwide provider of communications infrastructure solutions to enjoy a consistent, supportable infrastructure while taking advantage of new document-sharing, collaboration, and security features on the desktop. In particular, Enterasys support staff benefited from the Remote Desktop capabilities of Windows XP, reducing help-desk calls by 50 percent and increasing problem resolution on the first call by 25 percent.

For Chief Information Officer Len Couture and his colleagues, however, these client management benefits were only the beginning of what they envisioned for their deployment of Windows XP. The next steps were to take advantage of the synergies between Windows XP and Microsoft Windows Server 2003 for developing a comprehensive back-end solution to support the security requirements of the company. "Security is an essential component of the products we build and support, so it's equally essential that we implement a solid foundation of security internally," Couture says.

Solution

On its servers, Enterasys Networks upgraded from Microsoft Windows NT® Server version 4.0 and Windows 2000 Server to Windows Server 2003, Enterprise Edition (Release Candidate 1 and 2). On its PCs, Enterasys installed Microsoft Windows XP Professional Service Pack 1 and Office XP Professional Service Pack 2. The goal of these upgrades, according to Director of IT

Solution Overview

Customer Profile
Enterasys Networks is a leading worldwide provider of communications infrastructures for enterprise-class customers. Enterasys is headquartered in Rochester, New Hampshire.

Business Situation
Enterasys wanted a more manageable and secure environment, an easy way to deploy wireless access to consultants and contractors, and a better approach to configuration and lockdown.

Solution
Enterasys built on its deployment of Microsoft® Windows® XP Professional with the added functionality of Windows Server 2003 Active Directory® Group Policy for manageability and security.

Benefits
- Deployment of certificates for secure wireless access for users at offices worldwide in just two days
- A more manageable and secure environment with consistent server configuration and lockdown practices

Software and Services
Microsoft Windows Server 2003, Enterprise Edition, with Active Directory and Internet Authentication Service (IAS)
Microsoft Windows XP Professional
Microsoft Office XP Professional
Microsoft Consulting Services

Hardware
Compaq, Dell, IBM, Toshiba

Microsoft®

Operations Khalid Maletan, was twofold: "We wanted to boost the company's ability to meet the targets established for the original Windows XP deployment by reducing hard-disk images so as to ensure consistent configurations, and we wanted to apply manageable and secure standards to the building and operating of servers and desktops alike." Toward the third goal, the company is using Windows Server 2003 Internet Authentication Services for its primary authentication access-control environment and its certificate services."

As part of its drive for a more manageable and secure environment, Enterasys deployed Microsoft Systems Management Server for upgrading client PCs to Windows XP, applying hot fixes, pushing line-of-business applications to client machines, and rolling out Office XP Professional Service Pack 2. Enterasys also will use the Software Update Services Feature Pack to provide automated system-patch-level assessments for all servers and clients.

For all these deployments, Enterasys participated in the Microsoft Joint Development Program (JDP), which included Microsoft Consulting Services teams on-site and at Microsoft headquarters. Enterasys Technical JDP Lead Jared Weeks considers participation in the program indispensable. "By working in the Microsoft Joint Development Program, we were able to get our internal IT staff ahead of the game and have the assistance and guidance of Microsoft in adopting new technology early," he says. "We wouldn't have been able to deploy into production in a supported manner without it."
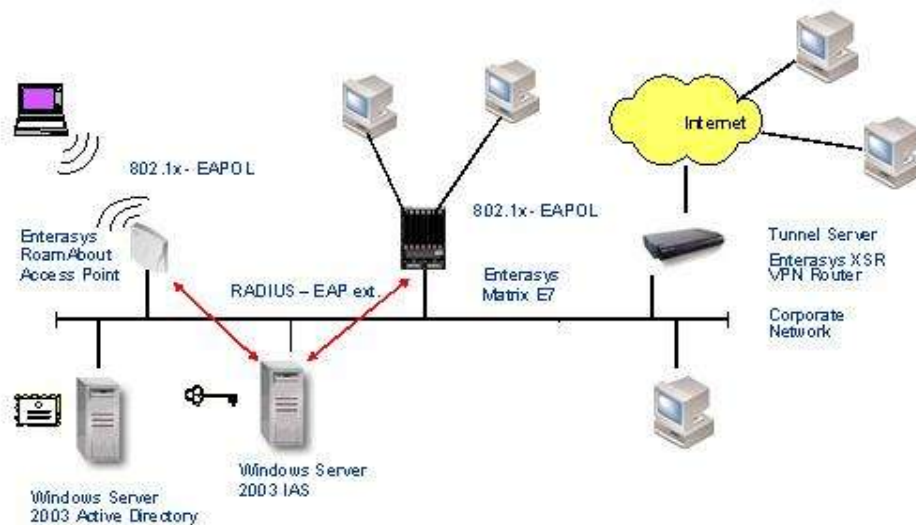
EAPOL = Extensible Authentication Protocol over LAN; RADIUS = Remote Authentication Dial-In User Service

Enterasys uses a public key infrastructure running on Windows Server 2003 for both wired and wireless users to access network resources through 802.1x authentication. Enterasys uses the same certificate infrastructure and Active Directory to provide virtual private network (VPN) authentication using Point-to-Point Tunneling Protocol (PPTP)/EAP and Layer 2 Tunneling Protocol (L2TP)/Internet Protocol Security (IPSec).

Microsoft

Benefits

Extending Wireless Access Quickly and Securely

For Enterasys IT executives, the ultimate goal for the corporate network was to increase security without increasing the administrative burden. They decided to achieve this goal by establishing a system for distributing Wired Equivalent Privacy (WEP) keys to clients securely and taking advantage of the Enterasys WEP rapid-rekeying function provided by the company's own RoamAbout R2 Enterprise Access Point product. To do this in a scalable and manageable way, the IT executives knew they would have to distribute keys dynamically and without user or administrative intervention.

So, with the help of the native 802.1x supplicant support in Windows XP, they implemented an enterprisewide deployment of 802.1x for all clients accessing the wireless LAN. 802.1x provides for both strong authentication (mutual authentication when using digital certificates) and secure, dynamic key management.

As part of that implementation, the executives selected the authentication credentials that they wanted to use from among those supported by Microsoft Windows Server 2003: EAP-TLS, which uses digital certificates for mutual (user and network) authentication, and Protected EAP (PEAP), which uses username/password credentials and a server-side certificate to authenticate the network. For Enterasys employees, a public key infrastructure (PKI) for EAP-TLS uses digital certificates for mutual authentication for services such as virtual private networking, Encrypted File System, and digitally signed e-mail. PEAP is used for users who do not have certificates such as vendors, partners, and consultants.

For implementation of the PKI, Enterasys took advantage of the autoenrollment capabilities available for Windows XP–based clients through the Microsoft Windows Active Directory® directory service and Group Policy feature in Windows Server 2003 to enroll user and machine certificates worldwide in just two days.

Manager of IT Operations David D'Abrosca explains that similar autoenrollment functionality existed in the company's prior Windows 2000 Server–based environment, but it required scripting and user intervention to ensure that users and machines automatically enrolled with the necessary certificates. "Having Windows Server 2003 on the servers and Windows XP Professional on the clients made all the difference," he adds. "It would have taken weeks to distribute the certificates had it not been for the new autoenrollment support available by having Windows Server 2003 and Windows XP."

By transitioning to 802.1x for all wireless LAN clients, Enterasys has positioned itself well for early adoption of the recently announced Wi-Fi Protected Access (WPA), the new security protocol that will effectively replace WEP as the security standard for Wi-Fi networks. With the current environment using 802.1x for the company's rapid rekeying, the transition to WPA will simply be a matter of upgrading the operating firmware on the access points to the WPA version and installing the Windows XP Service Pack that adds WPA support to the 802.1x supplicant in order to take advantage of the significant enhancements to data security provided by the Temporal Key Integrity Protocol (TKIP).

A related Windows XP–supported technology that is simplifying the implementation of secure wireless networks at Enterasys is the wireless zero configuration service. By detecting available wireless networks, eliminating the need for vendor-specific client utilities to control 802.11

"Thanks to the support of Windows XP for zero configuration, we saved between two and three person-weeks of technical resources on a recent 802.1x implementation of about 2,000 client machines."

Rich Casselberry
IT Operations Manager
Enterasys Networks

"Now that we're more centralized, we are striving toward a model in which any support person can address a problem at any office. The best way to do this is to ensure that systems are configured and locked down consistently, and Active Directory enables us to do just that."

Khalid Maletan
Director of IT Operations
Enterasys Networks

Microsoft

interfaces, and providing a single common interface for monitoring wireless LAN parameters, wireless zero configuration greatly simplifies installation and the user experience, according to IT Operations Manager Rich Casselberry. "Thanks to the support of Windows XP for zero configuration, we saved between two and three person-weeks of technical resources on a recent 802.1x implementation of about 2,000 client machines," he reports.

The Value of Consistent Configuration and Lockdown

Another advantage of the move at Enterasys to a Windows XP–based client environment with Windows Server 2003 on the server is the way in which Active Directory enables the company to configure and lock down servers in a consistent fashion. Maletan explains that this capability fits smoothly into the company's emerging IT philosophy. "In the past, our IT organization was decentralized and without a consistent approach to infrastructure rollout," he says. "Now that we're more centralized, we are striving toward a model in which any support person can address a problem at any office. The best way to do this is to ensure that systems are configured and locked down consistently, and Active Directory enables us to do just that."

For more information about Microsoft Systems Management Server, visit: http://www.microsoft.com/smserver/default.aspIn other plans, Enterasys will widen access to its network environment while maintaining manageability and security by establishing for Enterasys customers a forest based on Windows Server 2003. CIO Couture explains that, as a superset of domains, a Windows Server 2003–based forest holds a common schema defining objects, attributes, and configurations. "Implementing a Windows Server 2003–based forest will enable us to avoid the time-consuming process of creating cross-domain trusts for providing network access to external users," he says. "We'll also reinforce and extend the benefits that the company is enjoying from the migration to the Windows XP and Windows Server 2003 environment by offering network access to our key customers in a cost-effective manner while maintaining network manageability and enhancing network security."

Microsoft Windows XP Professional gives you the freedom to do what you want at home and at work—simply, reliably, and securely.

For more information about Microsoft Windows XP Professional, go to: http://www.microsoft.com/windowsxp/pro/

For more information about Microsoft Systems Management Server, visit http://www.microsoft.com/smserver/default.asp

For more information about Active Directory, visit http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp

For more information about PEAP, visit http://msdn.microsoft.com/library/default.asp?url=/library/en-us/eap/eap/protected_extensible_authentication_protocol.asp

For more information about Group Policy, visit http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp

Microsoft

For More Information

For more information about Microsoft products and services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Information Centre at (877) 568-2495. Customers who are deaf or hard-of-hearing can reach Microsoft text telephone (TTY/TDD) services at (800) 892-5234 in the United States or (905) 568-9641 in Canada. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information using the World Wide Web, go to:
http://www.microsoft.com/

For more information about Enterasys Networks products and services, visit:
http://www.enterasys.com/

Microsoft