

Asigurarea confidențialității datelor în rețelele private virtuale

Data Privacy Assurance in Virtual Private Networks

Ioan COSTEA

Smith&Smith Romania

nonicostea@yahoo.com

Abstract

VPN (Virtual Private Network) can be defined as a private connection between two stations or networks, established through an open public network. VPN technology allows a company to expand their services over the Internet, remotely, in conditions of maximum security. The VPN solution is suitable for companies that need secure and stable connectivity to applications and resources for an unlimited number of concurrent users. A VPN network is initiated around a security protocol that encrypts or decrypts data at the source and destination.

Index terms: network, VPN, privacy, security

References

- [1] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt and A. Warfield, “Xen and the Art of Virtualization”, 19th ACM Symposium on Operating Systems Principles – SOSP, 2003.
- [2] P.M. Chen, B.D. Noble, “When Virtual Is Better Than Real”, Proceedings of the 2001 Workshop on Hot Topics in Operating Systems, 2001.
- [3] P. Ferrie, “Attacks on Virtual Machine Emulators”, SYMANTEC ADVANCED THREAT RESEARCH, 2006.
- [4] R. Goldberg, “Architecture of Virtual Machines”, AFIPS National Computer Conference, New York, USA, 2006.
- [5] J. Kirch, “Virtual Machine Security Guideline”, The Center for Internet Security, 2007.
- [6] L. McLaughlin, “How to Find and Fix 10 Real Security Threats on Your Virtual Servers”, CIO, 2007.
- [7] Ș.V. Nicolaescu, “Aplicații în rețele virtuale private”, Buletinul AGIR, 2008.
- [8] M. Sabău, “Rețele virtuale private”, Net Report, noiembrie 2004.
- [9] R. Sailer, E. Valdez, T. Jaeger, R. Perez, L. Doorn, J. Griffin and S. Berger, “Secure Hypervisor Approach to Trusted Virtualized Systems”, IBM, 2005.