Chapter 23

CONTROLLING ACCESS

INTRODUCTION

In today's complex and constantly changing business world, employees, partners, customers, vendors and contractors all require different levels of access to different areas of the Local Area Network (LAN) at different times for different business purposes. As a result, enterprises must have business security solutions that provide detection and enforcement at every point of network access. To that end, enterprises need a comprehensive, strategic approach to access control. It sounds simple enough: who gets in and who doesn't. But the issues involved can be complex, and the threats are real and growing [1].

Consider this: more than 90 percent of the 530 companies polled in one industry analysts' survey admitted to security breaches. Not surprisingly, 82 percent of the enterprises identified external threats like hackers as a likely source of those breaches, but 77 percent of the enterprises also identified disgruntled employees as another likely source. That's why smart enterprises are not only focused on preventing unauthorized access but also detecting and enforcing policies at every point of access for all authorized users [1].

The number one issue is a general complacency that somehow a security breach, if it happens, will have a small impact on the enterprise. So many enterprises, even the larger, better-established enterprises, do not put enough resources into preventive strategy, and they spend an inordinate amount of resources when a disaster or problem hits [1].

However, a substantial number of enterprise networks still have vulnerabilities, including unprotected LAN ports that are easy prey for viruses, hackers and malicious users. The 2006 FBI/Computer Science Institute Computer Crime and Security Survey states that many enterprises simply do not know what's going on within their networks [1].

Those enterprises face substantial risk and have little chance of constructing an audit trail to find out how or why an incident occurred. But there is a better way [1].

The network edge is the place where users and applications connect, where traffic enters and exits the network, and where the network must determine how that traffic should be handled. The edge is where security policies can be enforced most effectively, where the

user gains access after being authenticated by a central command resource. This chapter explores how this comprehensive approach simplifies network access management, creates a secure, intelligent wired and wireless environment and provides affordable network security that detects all users and enforces all enterprise policies at every access point [1].

WHY ACCESS CONTROL?

When it comes to controlling access to their LANs, many enterprises leave their virtual doors open and their virtual windows unlocked, providing unrestricted access to a variety of end users. That lack of infrastructure presents little challenge to any malicious users and is one reason that 80 percent of enterprises surveyed in the 2006 FBI/Computer Science Institute Computer Crime and Security Survey reported internal security incidents [1].

The lack of access control measures also presents a huge liability for the enterprises. For example, in Fig. 23-1 [1], there are virtually no access control measures in place. A guest can access a LAN containing sensitive research and development information right from the enterprise's lobby or parking lot. The lack of access control measures can easily mean the loss of an enterprise's hard-won intellectual property or competitive advantage [1].

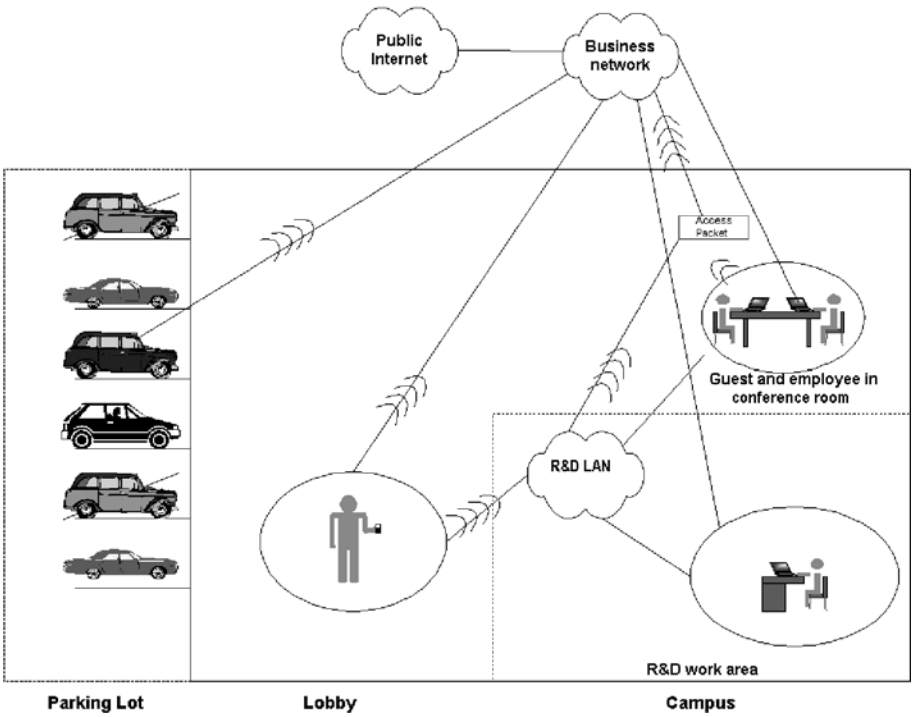

Figure 23-1. Common access control infrastructure.