Chapter 6
Securing Enterprises from Malicious Attacks on their Networks

Jameson Mbale
Copperbelt University, Zambia

Manish Wadhwa
Salem State University, USA

ABSTRACT

Routers interconnect networks of various enterprises, and the more secure the entry or exit points are made, the more robust the security of these enterprises is. These routers become the first direct targets and are vulnerable to security attacks. If these routers are not tightly protected, the attackers get an edge to intrude the system. In order to ensure the security of these routers, Secure Access Control Lists (ACLs) Filtering-Based Enterprise Networks (SAFE-Nets) are proposed in this chapter. In this scheme, routers are configured with Access Control Lists (ACL) that are used to filter in the intended packets and filter out the dangerous malicious packets from network traffic. This consolidates security deployment over the entire network on top of anti-virus software, weak passwords, latent software vulnerabilities, and other related secure measures. This can help network technicians working for various enterprises manage security at low costs.

INTRODUCTION

Businesses today depend upon various factors, but one major component that all businesses must pay attention to is how secure their online transactions are, how secure their servers are and how secure their network's entry and exit points are. Everyone is aware of Target's recent security breach. The reasons may be any, but the importance is of taking every measure to make one's networks secure. A big company loses millions or billions of dollars if it has to undergo security breach and it may take much less money if spent on making the networks robust and secure to begin with. There is always

DOI: 10.4018/978-1-4666-6473-9.ch006

a possibility of security being compromised for some reason or the other, but there should be every effort done in this direction.

Networks of various enterprises are connected through routers. It is thus important to make these routers, which are the entry and exit points for information exchange more secure. Malicious activities can be controlled through proper measures. In this chapter we discuss one such proposed model, *S*ecure *A*ccess Control Lists (ACLs) *F*iltering based *E*nterprise *Net*works, in this work abbreviated as SAFE-Nets. SAFE-Nets is envisaged to enhance the control of flow of malicious packets between the Enterprise networks. Routers, being the first devices connecting the network to other networks, they are the direct targets and vulnerable to security compromise by attackers. Attackers have repeatedly demonstrated their ability to compromise routers, through combinations of social engineering and exploitation of weak passwords or latent software vulnerabilities (Ao, 2003; Houle et al., 2001; Labovitz et al., 2001). The SAFE-Nets demonstrated in Figure 3 is composed of the layered network, routers and the Internet. The routers are configured with Access Control Lists (ACLs) that filter out the malicious packets, denying them to transverse across the network. In that way the network is free from being compromised by the malicious attackers.

Many Enterprises have invested a lot of resources in securing their computer systems from malicious attacks. They have acquired licensed anti-virus software to be used to protect and clean malware such as viruses, worms, trojans and many more malicious attacks, but still systems are prone to threats. Especially, the data, which comes from other networks linked by routers is vulnerable to such attacks. The routers link or connect two or more segments of networks. Once these devices are not properly protected, security between networks is vastly compromised and attackers get an edge to intrude the system. In fact, Thomas (2003) gave a scenario where one network operator recently documented over five thousand (5000) compromised routers as well as an underground market for trading access to them. He explained that manipulating, diverting or dropping packets arriving at a compromised router; an attacker can trivially mount denial-of-service, surveillance or man-in-the-middle attacks on end host systems. Such a scenario really entails how critical it is to secure the routers on the network. In relation to this, Mızrak et al., (2005) emphasized that network routers occupy a key role in modern data transport and consequently are attractive targets for attackers. From their expression, one clear emphasize is that when establishing and running a network, it is paramount to as well consider protecting the routers rather than relying only on securing anti-viruses. It is in view of this that the SAFE-Nets was envisaged to enhance the configuration of access control list into the routers in order to seal and consolidate the filtering out of the malicious in-out flow data between the networks. Once the in-out flow of malicious data is filtered out, the management of securing the information towards the end users would be controlled.

Nowadays people access their daily life information through Internet, particularly financial transactions such as: online banking, checking account balances, money transfers, online purchasing of goods, for example airline tickets, etc. However the hackers who temper with the online information and thus destabilize the whole corporate system have hampered such transactions. As discussed in the previous sections, one of the SAFE-Nets's key objectives or goals could be seen close to that of hackers which was to deny or prevent the particular identified information from flowing in the network. However, the critical difference of the two was that, the SAFE-Nets deny the malicious packets, whereas, the hackers prevent and paralyze the authorized packets disturbing the daily operation of the corporate systems. One of