Securing Your Network: Protecting Valuable Corporate and Intellectual Property in an e-nabled World

by *Ajay K. Sood,*
Nokia Internet Communications, Toronto, ON

Abstract

This document provides an introduction to the basic components of an Internet perimeter defense system. Security technologies such as Firewalls and Intrusion Detection Systems (IDS) are discussed, as well as the basic concepts of network security as well as the premise of risk assessment. A case study pertaining to the proliferation of the Code Red virus is detailed, as well as a brief look at future security technologies.

Sommaire

Ce document sert comme introduction aux composantes des systèmes de sécurité Internet. La discussion se centre autour des pare-feux (firewalls), ainsi que des systèmes de détection d'intrusion. En sus, les concepts fondamentaux par rapport a la securité informatique sont discutés. Finalement, une étude de l'epédimie informatique << Code Red >> est fournie, ainsi qu'un regard vers le futur de la sécurité informatique.

1.0 Introduction

The Internet has ceased to become an optional component to any company's business strategy. Rather, the Internet has risen to become an enabler for business, whether that business consists of effectuating commerce, business development, research and development, or other contemporary practices.

An emerging reality, however, is that there is a risk associated with this notion of integrating the Internet as part of one's business or research practices. Conventional as well as electronic media have been peppered with items recounting incidences of revenue losses, data theft, and more recently, 'cyber-terrorism', as politically minded hackers use their skills to make a statement.

2.0 The Role of Internet Security

The practice of Internet security is centered on the notion of risk mitigation, in that one can never be assured to the point of certitude that an Internet-enabled system is truly secured. Security consultants are frequently sought out in order to identify and classify information or assets at risk, enumerate these risks, and subsequently make recommendations to mitigate them.

The tools of the trade are numerous. Forensic tools such as scanners can be used for network discovery, and vulnerability identification, whereas customized data audits can be used to verify the security and integrity of data stores. The dichotomy of the situation is that these, and other tools are not only used by security professionals to obtain information, but also by hackers (those who make it their business to misuse, misappropriate, or corrupt information which is not theirs). What these two factions have in common is that they deal in acquiring information - it's what they do with it, which differentiates them.

The lesson then becomes, that the science of Internet security deals with the mitigation of the risk of having critical information compromised, and thus, having the cyclical processes in place to review, refine, and improve the status quo, so that critical assets and information are protected. That having been said, what are the key components of a secure network infrastructure?

3.0 Firewalls

Firewalls are a typical starting point for enforcing security policies on Internet Protocol (IP) networks. A firewall is a network traffic governor, which inspects and filters network traffic, which is incident on any one of its interfaces, much like a router with a security subsystem. The role of a firewall is to stratify a network infrastructure into domains of trust, by delineating zones, and regulating communication between them. The behaviour of a firewall should be a representation of the security policy, which it supports.

Practically, contemporary firewalls are so much more. Over and above merely filtering an IP packet based upon its OSI layer 3 parameters (source IP, destination IP, source and service ports), today's firewalls do not even live up to that name if there is not some form of state-derived inspection performed on these packet streams, which is to say that packet filtering is not enough. Packet inspection algorithms, which make decisions on whether or not to accept a given packet stream based upon previous traffic states, are now the norm.

A simple example is the establishing of a client-server TCP session through a firewall (the most common - like HTTP, FTP and SMTP), which takes place in three phases, each consisting of a single packet (Figure 1):

- The client SYN packet, which constitutes a client's proposal for communication,
- The SYN/ACK, which signals the server's readiness to transmit, and
- The client ACK, which signifies completion of session establishment - please continue.

Typical packet filtering technology (present on conventional routers, for example) would have to permit all three of the aforementioned messages in any given order, for this transaction to work, whereas a state-sensitive firewall would exercise more sophistication in this matter:

- The firewall would be configured only to accept a connection (SYN-request) to a given server (WWW server, for example), on a given service (in this case, WWW - port 80), from an arbitrary Internet client with IP address, say a.b.c.d,
- Once a qualifying SYN is received, the server would then be permitted to reply with its SYN/ACK,
- The firewall would record these occurrences in a state table, which would anticipate an ACK packet from a.b.c.d. Only this packet would be accepted, and no other packet from any other machine on the Internet would qualify,
- Once the ACK is received, the firewall will open a data channel between that particular client and the server, and record this instance in its state table,
- Exceptional cases (like a SYN without a SYN/ACK, or an order reversal) would not be passed, and
- Connection requests (SYNs) for any other service other than the ones prescribed (in this case WWW) would be blocked at the firewall.

4.0 Completing the Security Picture

So, while firewalls guarantee that only permitted IP addresses access private servers on the specified services, what is to stop the use of the inherent weaknesses in the accepted protocol? Recent events surround-

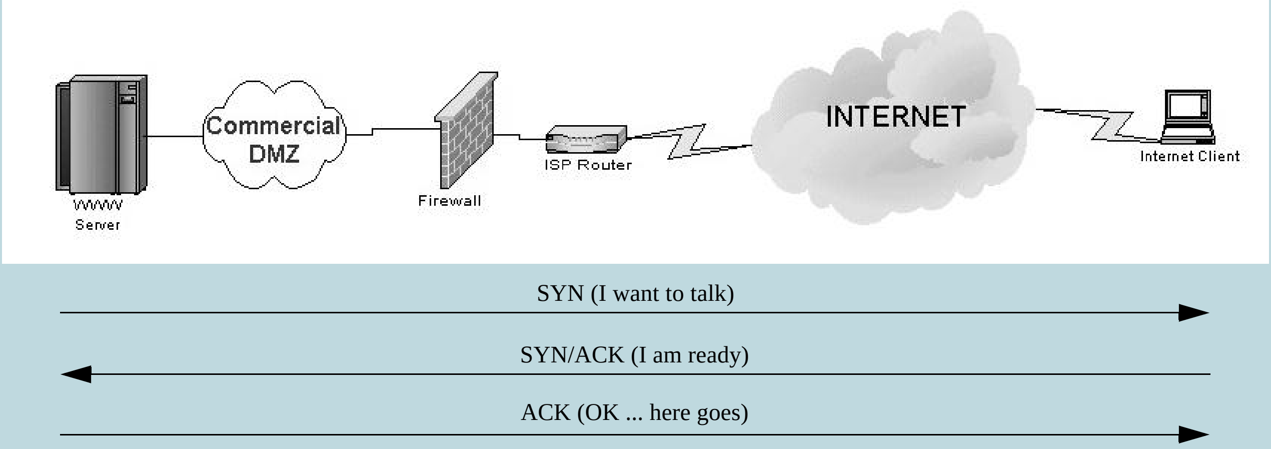

Figure 1 – The Client, the Firewall, and the Server

ing the proliferation of the Code Red worm/virus have provided a great example of firewalls being a necessary component of, but not sufficient as a complete security solution.

Code Red exploited a vulnerability in Microsoft's IIS Web server, which runs on a large number of Internet web servers. Even though a majority of these web servers were protected by firewalls limiting connections to the WWW port (port 80), the worm was able to utilize the open port to infect the host and propagate itself. The firewall never had a chance!

Enter intrusion detection systems (IDS) - a technology which, in real time, examines the traffic flow of data across a given network segment. An IDS sits on the network, and monitors for attack streams, which may be flowing on the segment, but is not an active member of the data path. Rather, an IDS passively listens and reacts in a variety of ways to attacks that it detects. Typical reactions are alerts sent by email, SNMP, or pager, and can even go as far as reconfiguring the nearest firewall to reconfigure itself to stop the attackers, or send port resets to the attacking machine to close the offending connections.

So in the case of Code Red, although the firewall could, in theory, allow the worm to infect the web server, the IDS would sense the attack pattern in the transmitted data stream, and take the prescribed action, neutralizing the threat by sending a port reset, canceling the connection, or instructing the firewall to close down all traffic from the attacking IP address for a finite or infinite period of time. In either case, some form of logging and alerting would also be a mandatory component of the IDS strategy (Figure 2).

Therefore, it can be said that a complete perimeter defense system could contain a variety of components, each complementing the overall security goals of the enterprise, with the firewall acting as the nucleus of this system. Conversely, encryption techniques for authenticating and privatizing communications can be employed in order to set up what is

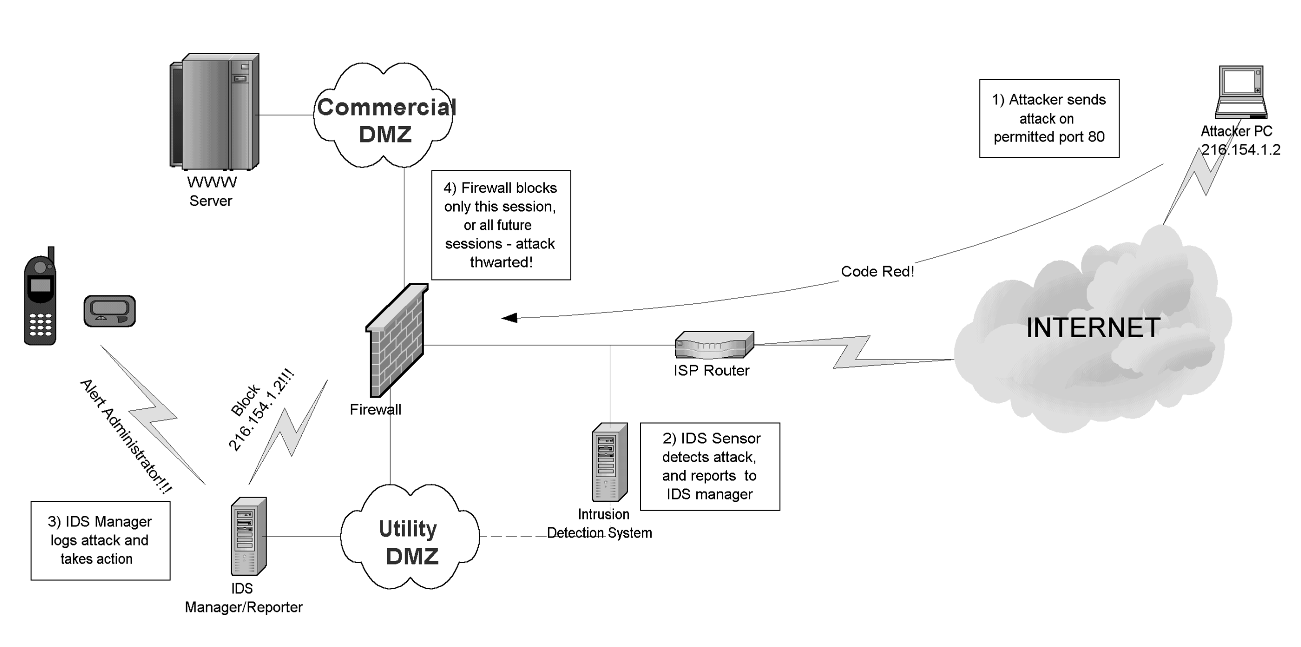

Figure 2 – Firewall with Intrusion Detection System

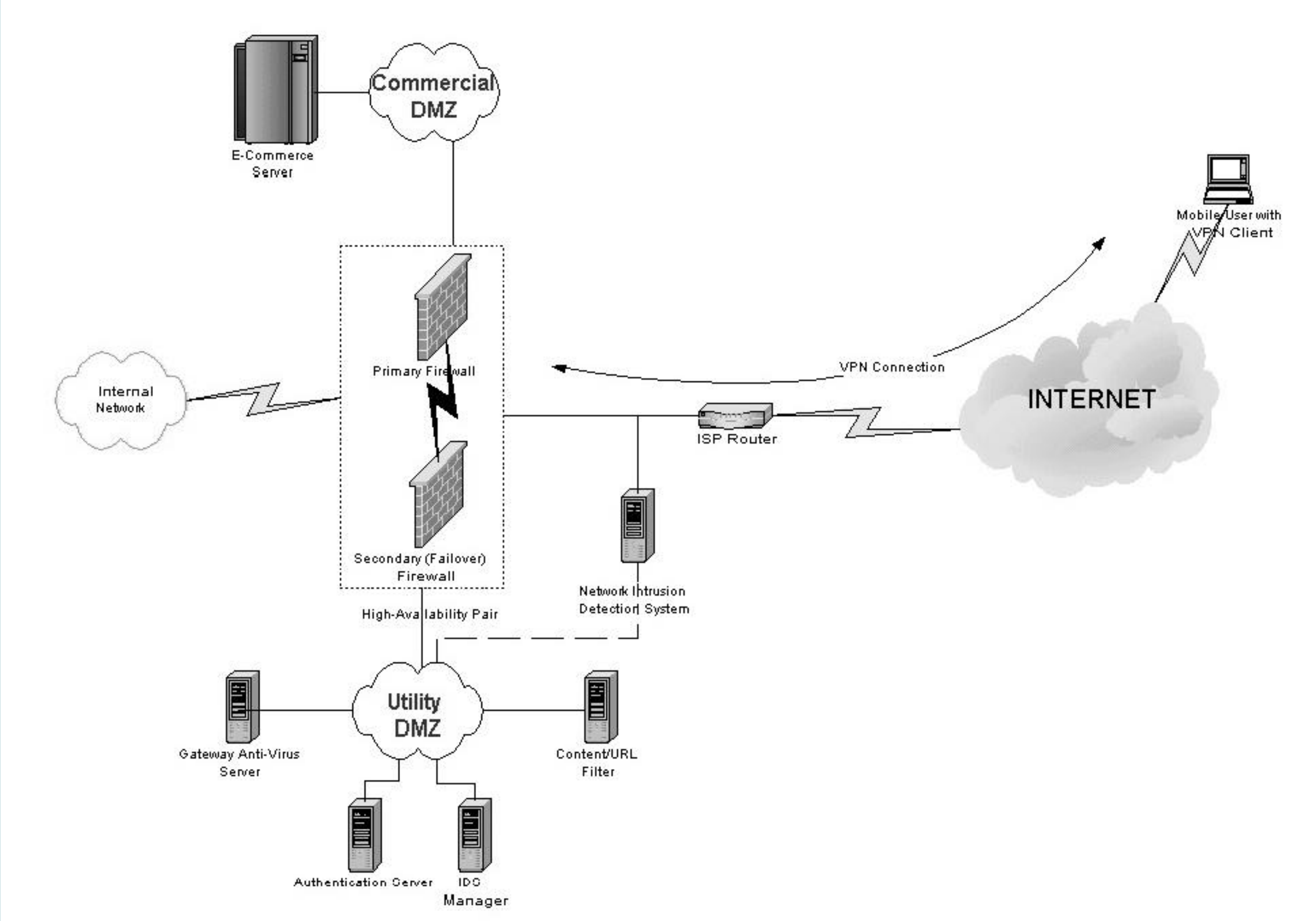

Figure 3 – Conceptual Security Infrastructure

known as a VPN (Virtual Private Network), connecting businesses across the Internet.

Additional technologies such as anti-virus gateways, or content filtering can be employed to inspect and control malicious content entering and exiting the enterprise. Authentication and non-repudiation represents again another exciting realm of security technology, with identifying technologies such as digital signatures, dual-factor authentication, and Public Key Infrastructures (PKI) all playing a role in certifying user identities (Figure 3).

5.0 Conclusion

In closing, it is important to note that information security should be regarded as an iterative process, with a cyclical nature. The Internet is an evolving landscape, and technology, as a whole, must adjust and scale accordingly. The advent of new technologies, network protocols, and practices will result in new ways of doing business. Emerging technologies such as mobile-IP will further enable a mobile Internet infrastructure, as we rush towards a mobile information society, in which a cellular handset/terminal will have a real IP address, a firewall and VPN client of its own, as well as a host of protocols, applications, and vulnerabilities.

Nokia Internet Communications (NIC), headquartered in Mountain View, California, is a leading manufacturer of Security appliances, including Firewall, Intrusion Detection, VPN, and anti-virus offerings. For more information about NIC, see:

http://www.nokia.com/securenetworksolutions.

6.0 List of Acronyms

DMZ	- De-Militarized Zone
FTP	- File Transfer Protocol
HTTP	- Hyper Text Transfer Protocol
IDS	- Intrusion Detection Systems
IP	- Internet Protocol
ISP	- Internet Service Provider
OSI	- Open Systems Integration
PKI	- Public Key Infrastructures
SMTP	- Simple Mail Transfer Protocol
SNMP	- Simple Network Management Protocol
TCP	- Transmission Control Protocol
VPN	- Virtual Private Network
WWW	- World Wide Web

About the author

Ajay Sood is a Sales/Systems Engineer at Nokia Internet Communications, and works with a variety of security technologies, such as firewalls, intrusion detection systems, virtual private Networks (VPNs), as well as authentication and anti-virus products. He has also served as a network security, design, and vulnerability assessment consultant for many organizations. Ajay holds a B. Eng. degree in Electrical/Computer Engineering from Concordia University. He can be reached at Ajay.Sood@Nokia.com