Global Information Assurance Certification Paper

Securing your network border-Essentials steps

Raul Zarate
April 4 2001

Introduction

Every company has felt the benefits of networking: faster internal processes, streamlined communications, increased productivity for telecommuters and mobile users, and the tangible achievement of a global market. Once a company taps the power of Internet commerce, virtual office resources, and instantaneous remote office feedback, the demand for access increases. Key trends driving the astounding growth of the Internet as a business tool include:

Increasingly Mobile Workforce

Businesses are relying more and more on a mobile workforce to remain competitive. The sales force needs to be able to access corporate files on demand.

Development of Extranets

Businesses increasingly need to interact on-line with their suppliers and business partners.

Need for an Alternative to Leased Lines

Previously, companies wishing to establish a private network have had no choice but to use a dedicated line, typically leased from the phone company. Recent research estimates that companies can save up to 70% over the cost of leased lines http://www.forrester.com

Security Risk Also Growing

The more complex networking becomes, the greater the challenge becomes to keep them secure. As your Internet and mobile computing infrastructure continues to expand, the access points into corporate data
from the Internet and dial-up phone lines multiply. Each access point represents a possible vulnerability that may be exploited to gain unauthorized entry into your network.

Threats from hackers have become legendary. The reality is even scarier – in a study by InternetWeek, 60% of respondents stated they have been penetrated over 30 times from the outside. http://www.internetwk.com

How can you ensure that only authorized individuals are accessing your information?

The first step is to formulate a security policy, identifying key assets to secure, and which assets you want to extend to whom. This process will help you establish specific security goals and a plan to tackle them. While this guide will focus on perimeter and Internet security, outlining the key security issues all networked company must address for safe connection to the Internet, realize you need a well-rounded strategy that encompasses the four categories of information security: Assess, Protect, Enable and Manage.

-ASSESS vulnerabilities and ensure policy compliance

-PROTECT critical information systems

-ENABLE secure Internet usage

-MANAGE and administer users and resources

Perimeter Security
Think of your corporate network as your fortress. To secure it against invaders, you must first build an impenetrable wall around it.

Step One: Secure the Perimeter with a Firewall
Your first line of defense within the enterprise is protecting access to and from the Internet. Without this protection, the door open to the Internet is also door open to the corporate network.

Types of Firewalls
There are three basic types of firewalls on the market today, each offering varying degrees of security and flexibility: routers, stateful packet filtering systems, and application-level proxy firewalls. A simple router, while inexpensive, is unacceptable for the vast majority of business needs. Routers cannot protect against network level attacks such as IP spoofing, source routing, TCP SYN Flood, Ping of Death and other such attacks not related to authorization of connections. Routers also do not provide the level of flexibility and features of a full-security enterprise firewall, such as virtual private networking capability, logging, and authentication. Stateful systems examine individual packets at or just before the network layer in the protocol stack. This speeds up rule-processing and prevents

packets not associated with an already established connection from getting through. In contrast, application-level firewalls authorize connections and examine the data stream by forcing all network traffic to be handled by an intelligent application running on the firewall system specific to the service (FTP, HTTP, SMTP, etc.). Such proxying gives you control over application-level functions and protection against application-level attacks, an absolute priority for almost all organizations. While many stateful systems include some limited proxy technology, most do not protect you against attacks embedded in the application stream, such as buffer overrun and illegal or unsafe application commands. Application-level firewalls, on the other hand, are designed to thwart the most sophisticated embedded attacks including those spanning multiple network packets.

Third Generation Security Proxies

Most of the stateful products have added security proxies - but without key features. The table below shows the differences between proxy generations. This is a gross approximation, meaning that some of the vendors will have some of the features in the next generation, but not all of them.

Generation	Typical Feature Set	Vendor Products
First Generation User Controls	Weak User Authentication Simple Logging Block all Java applets No connection transparency Non-transparent user authentication	CISCO PIX CISCO Centri Microsoft Proxy Server Network-1 Firewall/Plus Sun Sunscreen EFS-200
Second Generation User Controls Application Protections Ease-of-Use	Strong/Weak User Authentication Detailed Logging Command filtering URL Filtering Generic TCP Proxy Server-side transparency *(inside clients can appear to directly connect to external clients)* Non-transparent user authentication *(users must connect to firewall to get authenticated if user authentication is enabled)*	Checkpoint Firewall-1 DEC AltaVista TIS Gauntlet WatchGuard
Third Generation User Controls Application Protections Advanced Content Scanning More Ease-of-Use Performance	Strong/Weak User Authentication Detailed Logging Command Filtering URL Filtering with a rating database Integrated Finjan Java filtering/protections HTML verification and persistent HTTP connections HTTPs content verification – Strength of SSL verified Protection against buffer overrun attacks on HTTP and SMTP Multi-threaded architecture *(performance enhancement)* FTP within HTTP *(Implicit FTP using HTTP)* Transparent Proxy Redirection (send HTTP to another proxy)	AXENT Raptor Firewall

	More proxies (SQL*Net, SMB/CFIS, PING, H.323, etc.) Generic TCP and UDP Proxy Server-side transparency Client-side transparency *(servers on the inside can see the IP address of the client connecting to it)* Transparent User Authentication *(Users will be prompted to be authenticated without requiring them or their computers to be aware of the firewall)*	

Factors to Consider:

Address Translation and/or Hiding
Your firewall should be able to translate source and/or destination IP addresses from their original to a different address. The translation is required for a couple reasons. The first is to hide all the internal addresses of a network. Hiding the addresses ensures that would-be attackers have little or no information about your inside systems that could be used to attack them. Secondly, translation helps to conserve address space

Creation of Access Rules
The firewall follows a set of rules that you configure according to your security policy.

Speed/Performance
Your firewall acts as the gateway for all communications into and out of your corporate network, authenticating users, encrypting and decrypting messages, and routing these messages within your network. The firewall must tightly control security while handling traffic from hundreds of users without slowing down network traffic.

Authentication
Your firewall should be able to authenticate users attempting connection to your network.

Logging
A record of each connection that attempted to connect to or through the firewall. This would include both successful and unsuccessful attempts.

Alerting
Alerting is the mechanism to notify an administrator when the firewall needs attention.

Virtual Private Networking Capability
Virtual private networking capabilities allow distributed companies to extend the network beyond physical boundaries and provide secure communications to a mobile sales force or remote branch offices.

Content Blocking
Some firewalls offer integrated blocking mechanisms that allow you to restrict Web or newsgroup browsing of non-productive or objectionable material.

Step 2: Check Perimeter Security
Once the firewall is installed and configured, your next step is to test it out thoroughly to ensure you haven't left open or inadvertently created any compromising holes or weaknesses that could be exploited. Because networks are complex and constantly changing, such penetration tests should be performed on a routine basis.

Step 3: Install a Sentry
While a firewall will alert you of suspicious activity, it does nothing to stop it. Attempting to manually review log file is hopelessly time-consuming and a losing battle. Installing an automatic intrusion detector gives you an extra measure of protection.

Step 4: Prevent Unauthorized Access via Dial-Up
Preventing unauthorized access to your network is the final piece of perimeter security. Without authentication, a hacker can easily impersonate legitimate users to gain access to the corporate network. There are two basic types of authentication schemes being used by today's operating systems, communication servers, and firewalls:

- Static (hard-coded) password
- Two-factor (strong) authentication

Static passwords are too easily known by others, shared, guessed, and cracked.

Two-Factor Authentication
Two-factor authentication systems uniquely authenticate users without forcing them to remember another new password. Two-factor authentication is based on the proven principle of something unique that the user has -- a token -- and something unique that the user knows – a PIN number to activate the token. This process creates a unique one-time password that cannot be guessed, shared, or cracked. For that reason, two-factor authentication is highly preferable to other less, secure schemes.

Software vs Hand-held Tokens
While software and hand-held tokens are equally secure, each has its distinct advantages. Software tokens are ideal for users who employ a single device to log-on to the network, whereas hand-held tokens are best utilized by users who frequently log-on from many different computing locations and platforms. Hand-held tokens are easily lost or stolen and are twice the cost of software tokens. On the other hand, because software tokens are transparent to the user, they are easier to use. Additionally, they eliminate the need for users to carry a separate hand-held token. The user's laptop computer or PC becomes a token when the software token is activated.

Internet & Extranet Security
While the affordability and availability of the Internet make it an attractive business tool, it is a public network that offers no securityE-mail, files and passwords are easily intercepted by a variety of “sniffers” and hacker tools. To extend selective access to business partners, suppliers, and customers, without compromising security we need to:

Step 1: Implement a Virtual Private Network
A virtual private network combines authentication with data encryption and authorization to protect information en route over the public Internet. VPN technology:

1. Establishes a secure tunnel between the remote user and the corporate Network
2. Encapsulates and encrypts data packets
3. Authenticates the user and authorizes user access of the corporate resources on the network.

Encryption
Before transmission, the data is encrypted and encapsulated to protect it from prying eyes. Information can not be viewed, modified or intercepted in a usable form from these encrypted packets. Encryption using 56-bit Data Encryption Standard, or DES, algorithm are approximately 65,000 times stronger than 40-bit algorithms. Although there has been recent publicity about a successful, concerted Internet effort to crack a short DES message, for most purposes DES is considered to be very strong. For US and Canadian use, even stronger algorithms can be used. In general, these algorithms, such as Triple-DES, use longer key lengths to provide more protection.

Step 2: Identify Those Accessing Information
Virtual private networking products must provide a way of ensuring, or authenticating, the user's identity. Traditional authentication relies on passwords that are static or reusable.

Step 3: Remote Access Control
Remote users at multiple branch sites require the same security level as your corporate headquarters. That means fortifying their perimeter with a firewall, checking it routinely with a probe tool, and installing an intrusion detector for proactive response to intruders.

Step 4: Secure Remote Web Access
Companies are rapidly deploying Web-based applications as a convenient way of publishing information and accessing corporate services making it available in one central location. Your Web applications provide access to valuable company information and are visited frequently. Unfortunately, internal Web servers are critical resources that make good targets for internal hackers. Providing secure, centralized access control to Web-based information is particularly challenging given the limitations of today's Web technology.

Conclusions:
As a key part of the a security model the first step to proactively reduce corporate risk is to effectively measure compliance to a business security policy and assess vulnerabilities where critical information resides(**Assess)**.Then Organizations must protect information against unwanted users and hackers and control access to information to maintain business integrity. Balancing these needs requires a solution set that protects data from within the perimeter, checks and detects attacks to the perimeter and controls access to information to assure customers that proprietary data is secured(**Protect)**. The Internet is an essential resource that enables organizations to communicate more efficiently reduce telecommunication costs and provides more timely information(**Enable**).
.And finally effective secure solution to manage and administer users and the computing resources from one central location(**Manage**).

Source and references

1. 1.- Forester Reserch
   http://www.forrester.com/Home/0,3257,1,FF.html

2. Internetweek online .
   http://www.internetwk.com

3. Cisco Systems
http://www.cisco.com/public/products_tech.shtml

4. Checkpoint Firewall
http://cgi.us.checkpoint.com/rl/resourcelib.asp

5. Symantec Corporation
http://enterprisesecurity.symantec.com

6. Microsoft Corporation
http://www.microsoft.com/proxy/default.asp

7. Novell ,Border Manager
http://www.novell.com/index/products.html

8. WatchGuard technologies
http://www.watchguard.com/products