Abstract

Introduction to Network Security & Handbook for Firewall Implementation for Management

by Marc-André Laverdière

Computer security is an issue raised more and more by managers of businesses of all sizes, as this topic gets more and more media attention. This issue is multidisciplinary and an approach similar to concurrent engineering practices could be used to effectively secure data from prying eyes. A simple three-step approach can be used to address the problems and issues related to ensure efficient and budget-wise results. Also, a general overview of computer networks is presented in the appendices.

Key words:

- Methodology
- Concurrent Development
- Firewalls
- Computer Networks

Introduction to Network Security & Handbook for Firewall Implementation for Management

By Marc-André Laverdière

November 16th, 2000

Contents

List of Figures

Chapter 1

INTRODUCTION

As computer security becomes a major concern for organizations of all sizes, non-technical managers can be overwhelmed by technical decisions related to projects intended to secure corporate information.

Sometimes, management will not understand the major concerns that those topics imply, viewing only an unplanned expense ruining the budget.

Network security is about protecting assets. Even if the implementation costs for high-security systems seems to be fairly expensive, it is important to remember that it is only a small investment for the future of the organization.

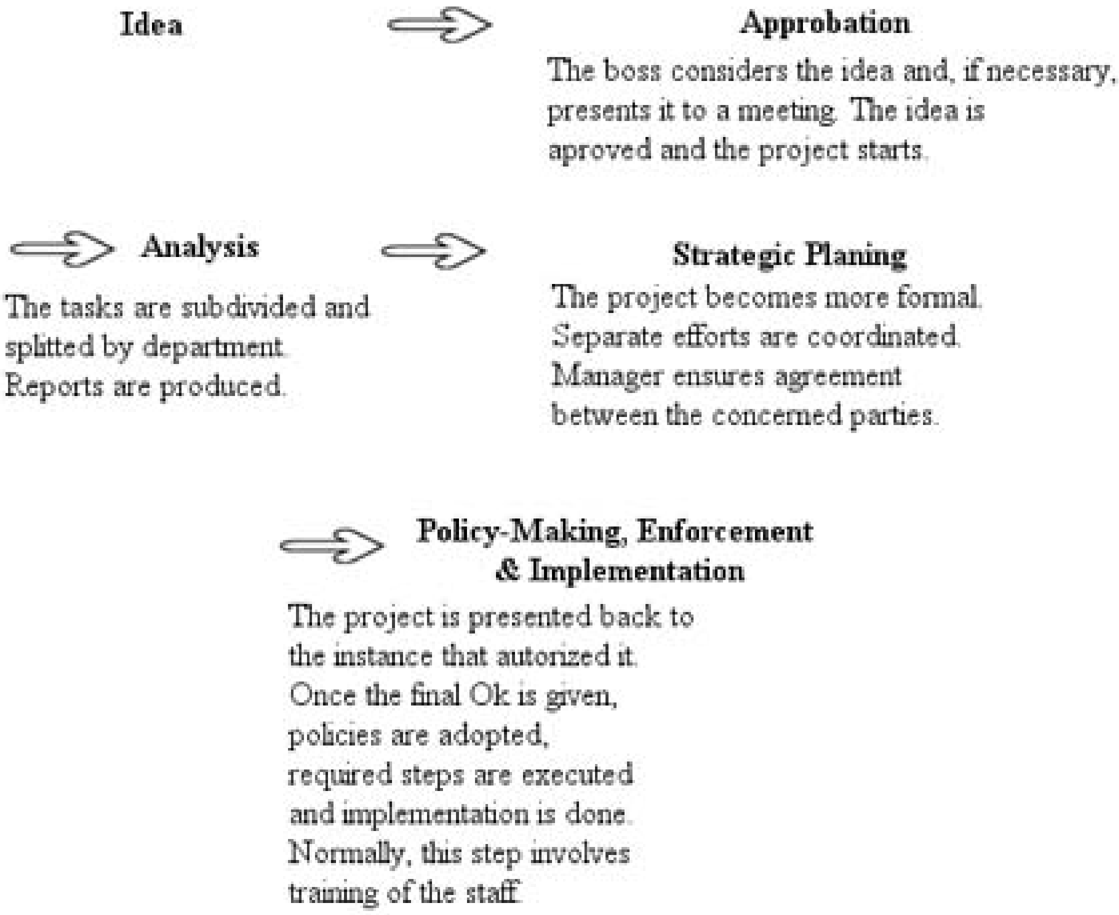
What is the cost for security? High.

What is the cost for doing nothing? Even higher [1].

If, due to inappropriate policies or inadequate network security, a hacker manages to obtain highly sensitive information - such as client information, projects in development, employees' personal files, etc - then the loss of confidence from business partners can ruin the bright future of any company [2].

Installing and maintaining a firewall system is only one step required for the safety of corporate data. Another major step is to make the users indulge in safe computing [3]. This security can only be truly reached by an approach similar to the process of concurrent engineering called concurrent development.

Such a project will normally go trough many phases. In this case, the management, the Human Resources Department, and the ITS will have to collaborate closely for the phases of Evaluation, Strategic Planning and Policy-Making, Enforcement & Implementation. (Please consult Figure 1.1 for an overview of the generic process)



Idea

Approbation

The boss considers the idea and, if necessary, presents it to a meeting. The idea is aproved and the project starts.

Analysis

The tasks are subdivided and splitted by department. Reports are produced.

Strategic Planing

The project becomes more formal. Separate efforts are coordinated. Manager ensures agreement between the concerned parties.

Policy-Making, Enforcement & Implementation

The project is presented back to the instance that autorized it. Once the final Ok is given, policies are adopted, required steps are executed and implementation is done. Normally, this step involves training of the staff.

Figure 1.1: Overview of the general Concurrent Development methodology

Chapter 2

STEP-BY-STEP DESCRIPTION

2.1 Evaluation

This stage of the project is crucial. All that is known before it is that the organization needs safety. After the evaluation, the organization will know what safety they need, what resources are ready and what steps and efforts will be needed for completion. (Figure 2.1 : Process of Evaluation details the those preparative steps)

At this moment, it can be useful to hire a consulting firm carefully screened for its capabilities. External feedback is usually the most constructive.

There are two aspects that will require more attention during this phase: the needs and the resources.

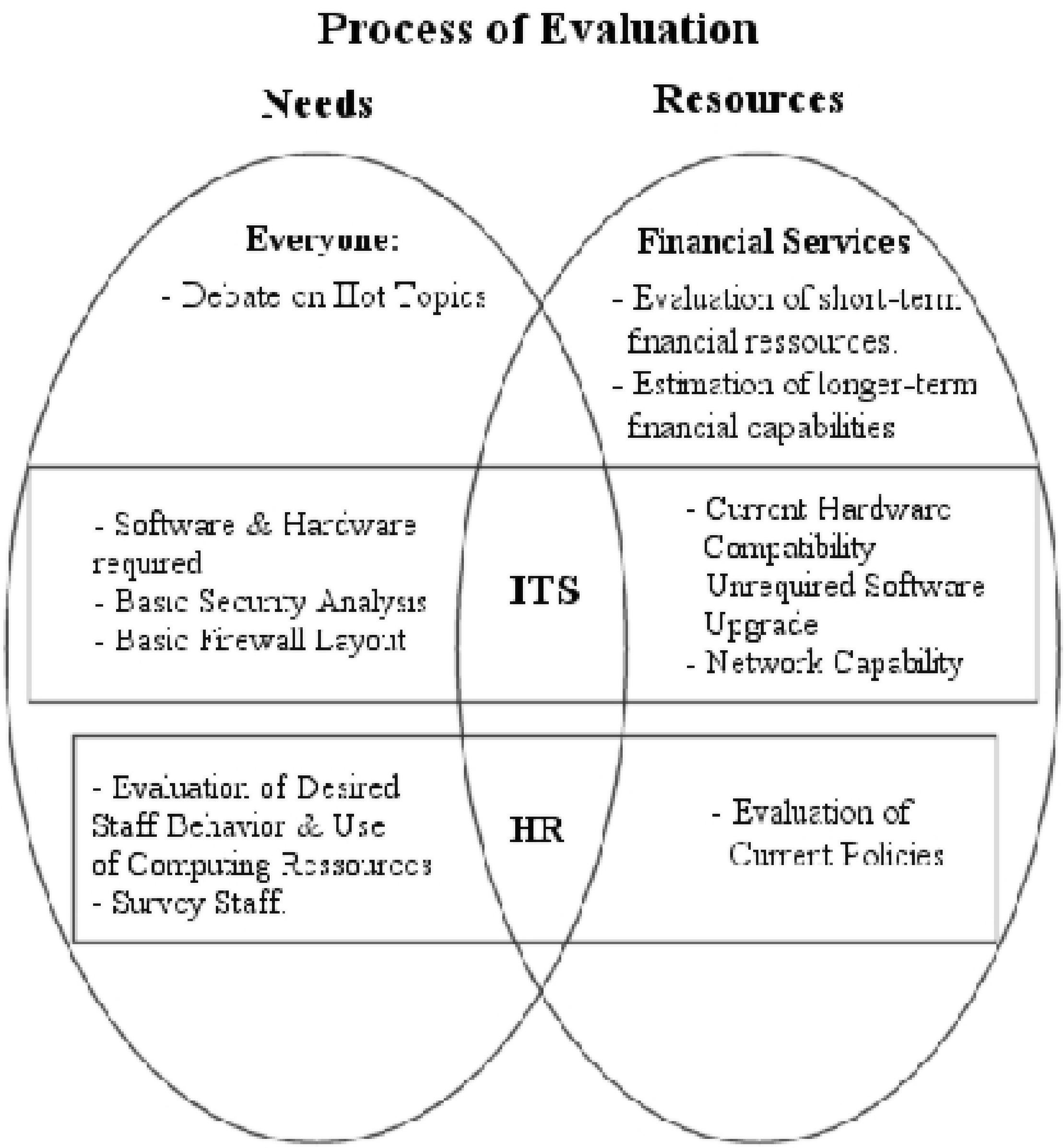

Process of Evaluation
Needs
Resources
Everyone:
- Debate on Hot Topics
Financial Services
- Evaluation of short-term financial ressources.
- Estimation of longer-term financial capabilities
- Software & Hardware required
- Basic Security Analysis
- Basic Firewall Layout
ITS
- Current Hardware Compatibility
Unrequired Software Upgrade
- Network Capability
- Evaluation of Desired Staff Behavior & Use of Computing Ressources
- Survey Staff.
HR
- Evaluation of Current Policies

Figure 2.1: Process of Evaluation

2.1.1 Evaluating the Needs

Many people will believe that this step is only done by the technical staff of the ITS, and that purely technical improvements should be regarded.

As said earlier, technical elements and ITS are only a part of the big picture.

At this moment, it can be useful to survey the staff and open up debates on their use of computing resources. Issues like file downloading, access restrictions, use of workstations, etc. have a terrible impact on overall security, and satisfying everybody is not easy [3]. With such an evaluation, it is easier to determine how to secure the organization's data from human weaknesses and to plan a strategy to circumvent social engineering practices as much as possible.

As firewalls can restrict access to specific sites, or even deny all access to all but a chosen few sites, this issue has to be debated even before the firewall layout is considered [4].

Another important issue to be discussed is monitoring. Now, the technology is sophisticated enough to allow monitoring of nearly everything on employee's workstations, from emails to each individual keystrokes. More and more firms do so, and apply severe consequences to employees violating the computing user policies [5] [6].

The ITS department should also take time to look at new software that could help employees use safer communications, especially in the case of representatives using notebook computers.

2.1.2 Evaluating the Resources

With massive amounts of money, there is not much you cannot do in the technological world.

It is important to assess the corporate resources, but not only on a financial level. The carefully evaluating the staff's technical abilities, as well as their personal capabilities, can make a difference between success and a project over budget and behind schedule. This will also help to identify leaders and motivated personnel as key players in the project. By giving more room and/or responsibilities to these persons, the project can become far more dynamic and stimulating for the rest of the staff, a very positive side effect.

This will also help when making major decisions like hiring and purchasing. If the need is evaluated sooner rather than later, integration of new personnel and equipment in the current flow of operations is unlikely to create a stressful situation for the rest of the employees. Obviously, it would not be useful to realize such a need during the implementation phase...

If short-term resources tend to be limited, then the planning will have to take this into consideration, maybe even delaying certain parts of the implementation or re-evaluating the schedule entirely.

Technological resources are as important, since older machines can cause unexpected problems during implementation and could require replacement.

2.2 Strategic Planning

Now that the key players are identified, the resources are known and that the needs are clear, a good view of the situation is available.

As clearly shows Figure 2.2, strategic planning is an exercise of teamwork. At this moment, key players and good employee relations will certainly make all the difference between a purely technical improvement and an overall solution. Now comes the time when strong leadership is needed and the nomination (even if informal) of the project coordinator(s) should be done.

This phase is based on concertation, as all departments will come to the table with their own view of the project. This is an opportunity to discuss the others' ideas, to set restrictions, to update the list of needs and resources, to improve proposals with constructive feedback, etc.

It is important to work on ”worst-case scenarios”. By analyzing what can go wrong, the schedule can be modified to be more adaptable to unplanned surprises by leaving room for adjustment.

At this moment, in the maelstrom of papers, ideas and figures, the need to write down clear and detailed specifications and schedules is present and generally overlooked. By putting on paper all the requirements, and by making all the parties involved agree with them, a project is born.

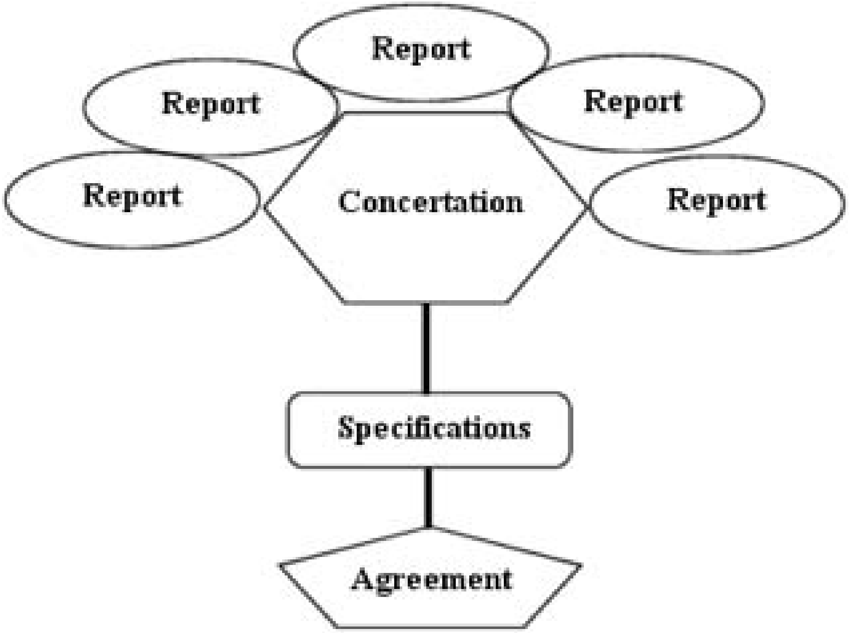


Figure 2.2: Strategic Planning

2.3 Policy-Making, Enforcement & Implementation

Earlier in the project, a good evaluation of the existing policies has been made, and specifications have been established.

Now, it is time to design policies to reflect the new realities on data security. Please consult Figure 2.3: Parallel Implementation, on page 11, for an overview of the actions.

The weakest link of a chain is the strength of the chain. No matter how well protected the systems and the information are, if employees are not trained properly to deal with technicalities and the new policies, then the money invested overall to secure the system is wasted. If a hacker wanting to get hold of specific data is unable to break through the systems, one has just to take the phone and indulge in some social engineering. The results are quite impressive.

The importance of strong policies on accounts and data access cannot be explained enough. Sometimes, employees will give dial-up and account information to friends or family members. This information could be used for less legitimate purposes than simple Internet access for kids during lunchtime, and hackers know how to profit from those weaknesses. With strong education and by attaching a financial value to security, risk of human-made security holes will greatly be diminished [3].

An educated staff is a more responsible staff. At this moment, it is important to develop seminars for the non-technical personnel to explain the issues and to introduce the technology as well as to clarify all the details. Also, it is good that ITS prepares documentation. Some staff members can be curious and may want to find out more about the technologies used.

Making the staff sign the new policies and answering questions can help the implementation on the human side [4]. Disciplinary measures and fines should be detailed to the staff so that everybody clearly understands that data security is a major issue that requires an effort from everybody.

This step should begin just before technical implementation, to avoid bad surprises. Employees will be aware that things are going to change in the short term and will have the time to assimilate the information for application. The change itself can help motivation and questions with good answers remove confusion that could otherwise lower productivity in such projects.

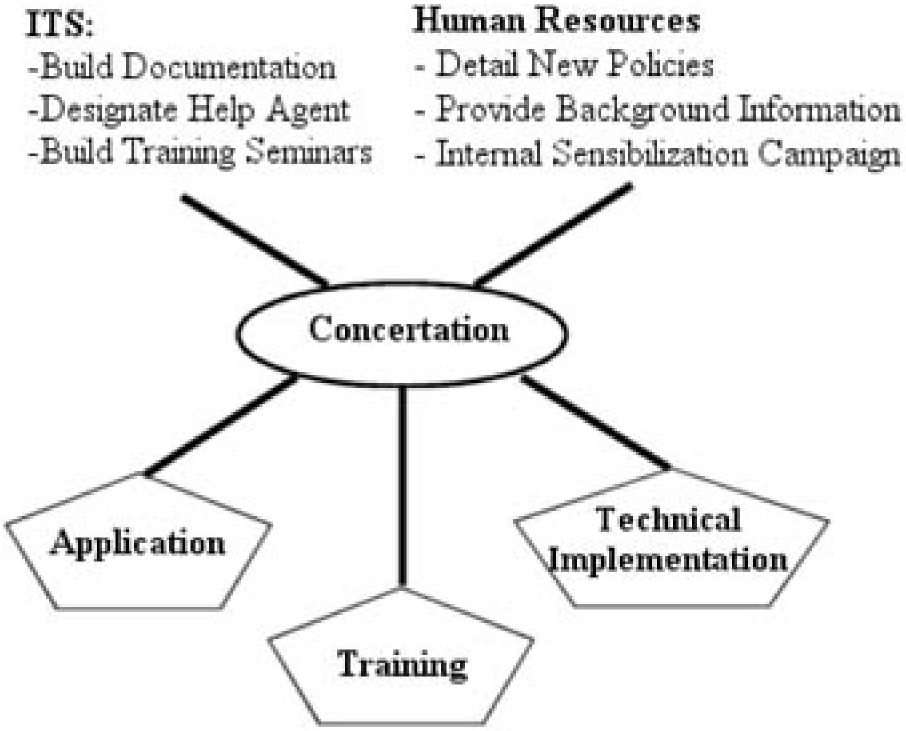


Figure 2.3: Parallel Implementation

Chapter 3

CONCLUSION

The issue of computer security is as technological as it is human. While vicious hackers will try to invade critical systems to take over information using the most developed tools and semi-arcane knowledge, cyber-vandals can use the staff to attain their goal.

This process of evaluation - planning - implementation using concurrent development methods can also be used on all kinds of projects and has demonstrated its flexibility and efficiency. The key of this process is returning the responsibility to the staff and energizing the organization on all levels.

Important issues such as employee monitoring are raised during the process and must be addressed diligently. Even if technologically possible, using extremely restrictive policies on access to the internet and corporate resources can only hurt in the long run, as an environment too restrictive will choke productivity and innovation. Securing from the staff does not imply a repressive approach, but a very formative one.

Chapter 4

References

[1] Louis-Éric Simard, network & systems security consultant, in interview on Nov. 6th, 2000

[2] Sandra Mingail, ”A need to circle the wagons”, Financial Post, Tuesday, Oct. 3rd, 2000, p.E2

[3] Michael J. Assels, Manager of Systems, Networks & Security; Department of Computer Science of Concordia University, in Interview on Oct. 19th, 2000

[4] Mike Pytlik, ”Internet policies”, Credit Union Magazine, July 1999, pp. 98-99

[5] David Noack, ”Nearly a Third of Firms Monitor Workers Online”, APB-news, Nov. 11th,1999 Available online at:
www.apbnews.com/safetycenter/business/1999/11/11/vaultsurvey111_01.html

[6] Paul Van Slambrouck, ”Conflict looms over the right to monitor e-mail”, Financial Post, Tuesday, Oct. 3rd, 2000, p.E13

[7] Marcus J. Ranum, Thinking about Firewalls, Glenwood, Maryland, Trusted Information Systems, Inc. Available at: ftp://ftp.tis.com/firewalls

[8] Jerry. Ablan & Scott Yanoff, Web Site Administrator's Survival Guide, Indianapolis, IN, Sams.net Publishing, 1996, pp. 320-327

[9] Marcus J. Ranum, An Internet Firewall, Washington, Maryland, Washington Open Systems Resource Center, Digital Equipment Corporation, 1992.

Note: some images made by the author used elements from [9] and from

- Marcus J. Ranum, A Network Firewall, Washington, Maryland, Washington Open Systems Resource Center, Digital Equipment Corporation, 1992
  Available on the web at: ftp.greatcircle.com/papers/ranum

- Avolio & Ranum, A Network Perimeter With Secure External Access, Glenwood, Maryland, Trusted Information Systems, Inc.
  Available on the web at: ftp.tis.com/firewalls

Appendix A

Glossary

Concurrent Development:

Terminology developed by the author. The core element is the decentralization of the tasks at hand. The objectives are, in order: satisfaction of all parties involved, increase of staff morale, involvement in the organization and diminution of development costs.

Concurrent Engineering:

Method of development using a systematic approach intended for manufacturing to develop products with respect of each department (i.e. Manufacturing, Technical Support, Training, Repairs, etc.) for better customer service and shortening development time.

Dial-Up:

Remote network connection through a modem and a phone line. This is usually the Achilles' foot of many networks.

Firewall:

Software or machine used to block access to specific computing resources. Please consult Appendix B for more details.

Hacker:

Person that uses computing skills or tools to break into computer systems.

ITS:

ITS stands for Information Technology Services. ITS is a department specialized in various networking and computing services and facilities.

In some organizations, these services will be managed by the Human Resources department or will be referred to as Computing Services.

Social Engineering:

Far from engineering, this is a method used to obtain information through social methods. Generally, it involves a malevolent person trying to convince an employee to deliver information for 'authorized' uses. This is the strongest tool of the hacker.

Appendix B

Notions of Computer Networks

Workstation:

Computer used in order to accomplish work on the personal level

Server:

Computer holding resources or services for the other computers of the network.

Network:

Method to allow computers to share information together. In order to communicate effectively, computers need to have physical connection between them and to share a protocol to exchange information. (see Figure B.1 on page 18 for an example.)

Router:

Computer or hardware built to redirect traffic from one network to the other. A router can also analyse traffic and deny some access. This kind is called a filtering router and is part of the firewall family [7].

Gateway:

Computer that sits between two networks. Each network is able to see the gateway, but unable to see through the gateway. Like the router, the gateway is responsible to ensure the transfer of data from one network to the other [7].

Proxy:

Gateway that hosts a caching program that keeps a local copy of popular network resources. By that caching, network performance is increased [8].

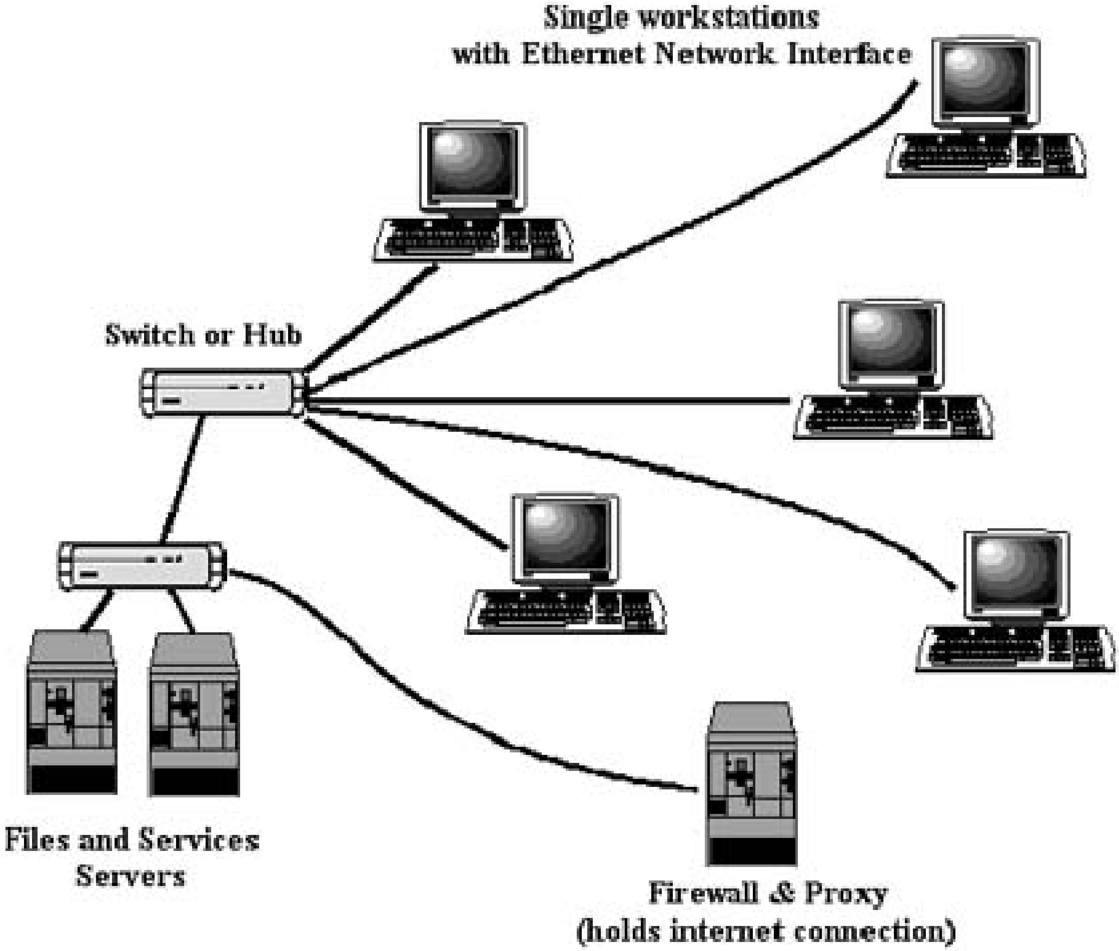


Figure B.1: Example of low-cost secure network implementation.

Proxy Firewall (Screened Host Gateway):

Gateway that holds a filtering program that is more advanced and secure than the router. There exist many vendor software and many devices built in order to complete that task. (consult Figure B.2 on page 19 for description of the gateway.)

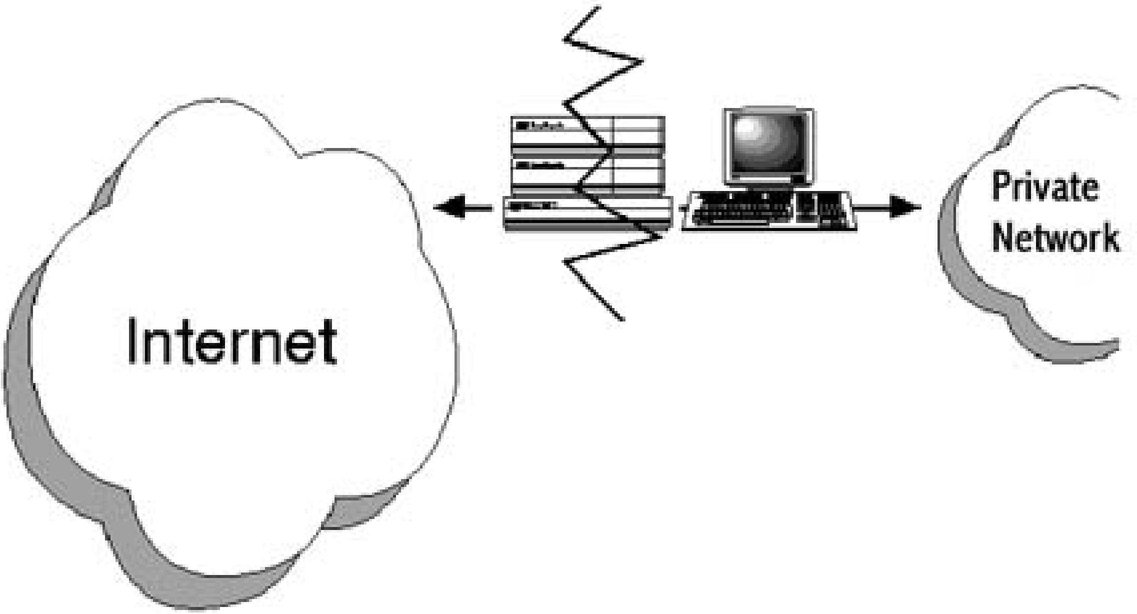


Figure B.2: Concept of the screened host gateway. The direct traffic is cut between the Internet and the network and filtering is applied [9].

VPN:

Stands for Virtual Private Network. This is a technology that uses a special 'tunnelling' protocol that allows a remote computer to access network resources through the internet like if that computer was inside the network. It features encryption and authentification for higher security in the communication. (Please consult Figure B.3 on page 20 for an overview of VPN cost-saving capabilities

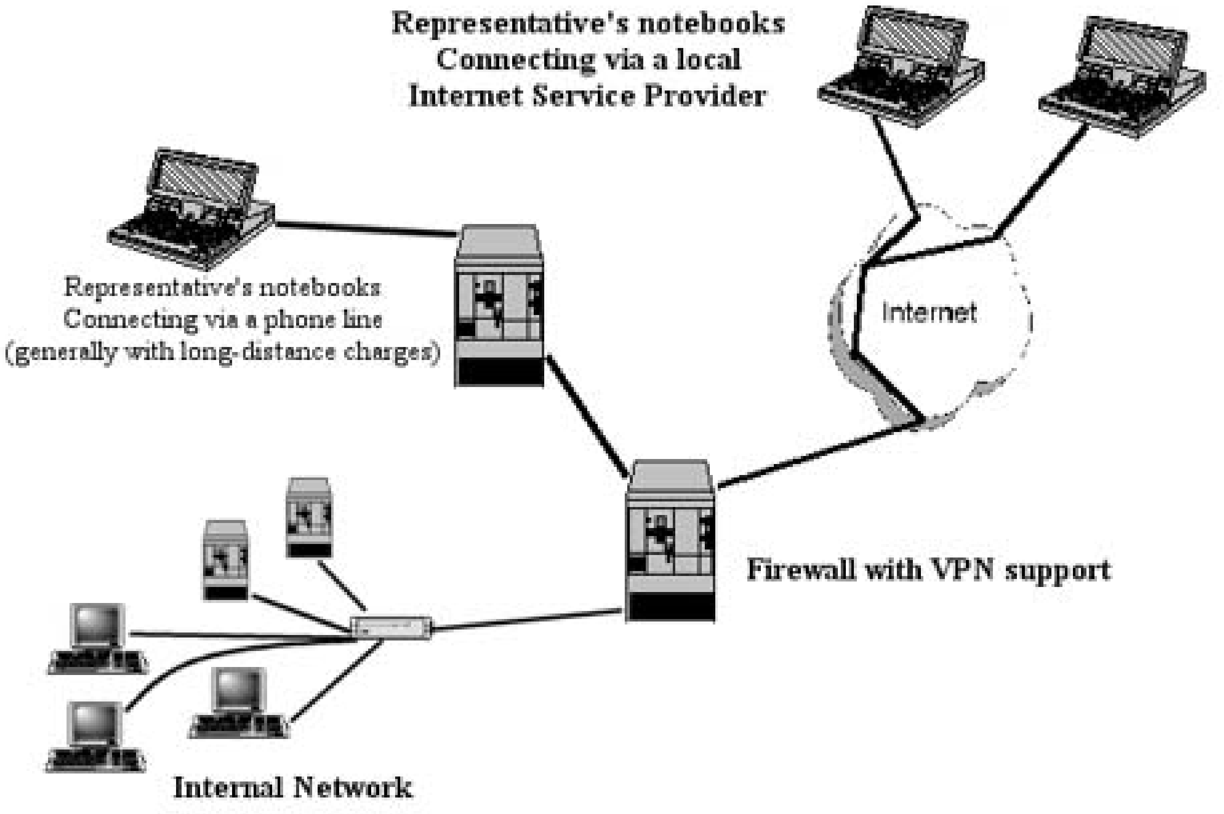

Representative's notebooks
Connecting via a local
Internet Service Provider
Representative's notebooks
Connecting via a phone line
(generally with long-distance charges)
Internet
Firewall with VPN support
Internal Network

Figure B.3: Overview of VPN cost-saving capabilities. Dial-Up access is no longer required, eliminating multiple security holes, and communication fees for road warriors are reduced.