DESIGN AND IMPLEMENTATION OF SYSTEM AND NETWORK SECURITY FOR AN ENTERPRISE WITH WORLDWIDE BRANCHES

Seifedine Kadry, Wassim Hassan

School of Engineering, LIU, Beirut, Lebanon

E-mail: skadry@gmail.com

ABSTRACT

The basic reasons we care about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, the if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

Another issue that is emerging in e-commerce is that good security can finally be seen as part of the market development strategy. Consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. We no longer have to look at security purely as loss avoidance: in today’s marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line. Networks today run mission-critical business services that need protection from both external and internal threats.

In this paper we proposed a secure design and implementation of a network and system using Windows environment. Reviews of latest product with an application to an enterprise with worldwide branches are given.

Keywords: *Network design, LAN, WAN, Security, Encryption, VPN, IPSec, Active Directory*.

1. INTRODUCTION

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms [8].

Governments, military, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on Privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of gaining entry into the field. It offers many areas for specialization including Information Systems Auditing, Business

Continuity Planning and Digital Forensics Science, to name a few.

2. SECURITY SERVICES AND PROCESSES

Security is fundamentally about protecting assets. Assets may be tangible items, such as a Web page or our customer database — or they may be less tangible, such as our company's reputation.

Security is a path, not a destination. As we analyze our infrastructure and applications, we identify potential threats and understand that each threat presents a degree of risk. Security is about risk management and implementing effective countermeasures.

- **Authentication**

Authentication addresses the question: who are you? It is the process of uniquely identifying the clients of our applications and services. These might be end users, other services, processes, or computers. In security parlance, authenticated clients are referred to as *principals*.

- **Authorization**

Authorization addresses the question: what can you do? It is the process that governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with system-level resources such as registry keys and configuration data. Operations include performing transactions such as purchasing a product, transferring money from one account to another, or increasing a customer's credit rating.

- **Auditing**

Effective auditing and logging is the key to non-repudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction. For example, in an e-Banking system, non-repudiation mechanisms are required to make sure that a client cannot deny ordering to pay a bill from his account.

- **Confidentiality**

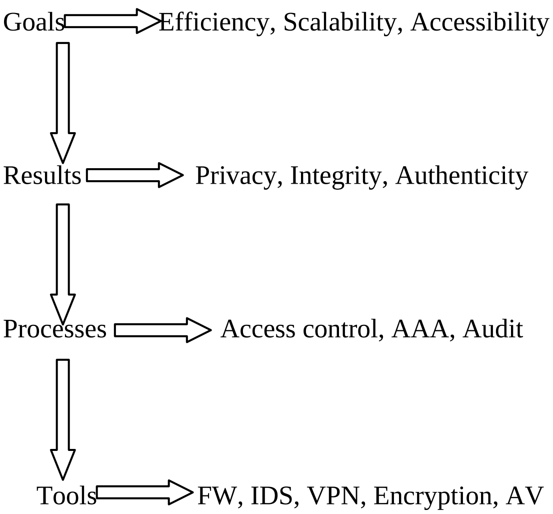
Confidentiality, also referred to as *privacy*, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is frequently used to enforce confidentiality. Access control lists (ACLs) are another means of enforcing confidentiality.

- **Integrity**

Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks. Integrity for data in transit is typically provided by using hashing techniques and message authentication codes.

- **Availability**

From a security perspective, availability means that systems remain available for legitimate users. The goal for many attackers with denial of service attacks is to crash an application or to make sure that it is sufficiently overwhelmed so that other users cannot access the application.


Goals
Efficiency, Scalability, Accessibility
Results
Privacy, Integrity, Authenticity
Processes
Access control, AAA, Audit
Tools
FW, IDS, VPN, Encryption, AV

3. WAN PROTECTION

All companies should protect its wide area network 'WAN' to make the connections between all their branches secure, and all sending data reach in safe hands as recipients. To let the external network of any company protected and high level secured, the virtual private network 'VPN' is a good solution to organize a secure access to the internal network remotely. Internet protocol security 'IPSec' is configured with VPN to have more security to the network. The encryption is a good process to support the communication to be secret by using a private key.

3.1 Virtual Private Network 'VPN'

One of the most important solutions to viruses and hackers threats is VPN [4] that makes the network between companies and users secured; it is also authenticated and encrypted for security. VPNs provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line. Basically, a VPN is a private network that uses a public network "usually the Internet" to connect remote sites or users together. Instead of using a dedicated, real world connection such as leased line, a VPN [11] uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

Three types of tunneling or encryption protocols that Windows Servers use for secure communication: L2F, L2TP and PPTP.

Layer 2 Forwarding ”L2F”: it creates network Access Server (NAS), initiated tunnels by forwarding Point-to-Point (PPTP) sessions from one endpoint to another across a shared network infrastructure.

Because L2F is not client-based, systems do not need L2F client software of configuration. However, this also means that communications between the users, systems and the ISP are completely unprotected. L2F can use authentication protocols such as RADIUS and TACACS+. However L2F does not support encryption.

Layer 2 Tunneling Protocol “L2TP”: it is IETF standard tunneling protocol that tunnels PPP traffic over LANs or public networks. L2TP was developed to address the limitations of IPSec for client to gateway and gateway to gateway configuration, without limiting multivendor interoperability. In these configurations, all traffic from the client to a gateway, and all traffic between two gateways is encrypted. L2TP uses its own tunneling protocol, which runs over UDP port 1701. Because of this, L2TP may be easier to pass through packet filtering devices than PPTP. L2TP can support multiple sessions within the same tunnel.

Point-to-Point Transfer Protocol “PPTP”: it provides a protected tunnel between PPTP enabled client "personnel computer" and a PPTP enabled server. It is not a standard tunneling protocol. It employs Microsoft Point-to-Point Encryption (MPPE) for data encryption. Microsoft developed PPTP, which like L2TP, tunnels Layer 2 PPP traffic over LANs or public networks. Microsoft has also created MS-CHAP to provide stronger authentication than PAP and CHAP.

PPTP creates client-initiated tunnels by encapsulating packets into IP datagrams for transmission over the Internet or other TCP/IP based networks. So L2TP is more secured than PPTP.

VPN services for network connectivity consist of authentication, data integrity, and encryption [11]. The two basic VPN types are remote access and site-to-site:

- **Remote Access**: Remote access VPNs secure connections for remote users, such as mobile users or telecommuters, to corporate LANs over shared service provider networks.

There are two types of remote access VPNs:

- Client Initiated. Remote users use clients to establish a secure tunnel through a shared network to the enterprise.
- NAS Initiated. Remote users dial into an ISP Network Access Server (NAS). The NAS establish a secure tunnel to the enterprise private network that might support multiple remote users initiated sessions.

- **Site-to-Site**: The two common types of site-to-site VPNs (also known as LAN-to-LAN VPNs) are intranet and extranet. Intranet VPNs connect corporate headquarters, remote offices, and branch offices over a public infrastructure. Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a public infrastructure.

3.2 IPSec

IPSec [3] is defined as a set of standards that verifies, authenticates, and encrypts data at the IP packet level. It is used to provide data security for network transmissions. IPSec is a suite of protocols that allows secure, encrypted communication between two computers over an unsecured network. It has two goals: to protect IP packets, and to provide a defense against network attacks.

Depending on which protocol is used, the entire original packet can be encrypted, encapsulated, or both. IPSec consists of a number of protocols. The two IPSec protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP), see the table (table 1) below:

Protocol	*Requirement*	*Usage*
AH	The data and the header need to be protected from modification and authenticated, but remain readable.	Use for data integrity in situations where data is not secret but must be authenticated — for example, where access is enforced by IPSec to trusted computers only, or where network

		intrusion detection, QoS, or firewall filtering requires traffic inspection.
ESP	Only the data needs to be protected by encryption so it is unreadable, but the IP addressing can be left unprotected.	Use when data must be kept secret, such as file sharing, database traffic, RADIUS protocol data, or internal Web applications that have not been adequately secured by SSL.
Both AH and ESP	The header and data, respectively, need to be protected while data is encrypted.	Use for the highest security. However, there are very few circumstances in which the packet must be so strongly protected. When possible, use ESP alone instead.

Table 1: IPsec Protocols

It is recommended that using L2TP/IPSec with certificates for secure VPN authentication. By using Internet Protocol security (IPSec) authentication and encryption, data transfer through an L2TP enabled VPN is a secure as within a single LAN at a corporate network.

The VPN client and the VPN server must support both L2TP and IPSec. Client support for L2TP is built in to the Windows XP remote access client, and the VPN server support for L2TP is built in to the Windows Server 2003 family. L2TP server support is installed when you install the Routing and Remote Access Server Setup Wizard, L2TP is configured for five or 128 L2TP ports.

3.3 Encryption

Encryption is one of best processes of encoding a message or data through a mathematical key in a manner that hides its substance from anyone who does not process the mathematical key. However, encryption has not always been applicable to network security. Traditionally, encrypting data for transmission across a network required that the same encryption key, called a shared secret or a private key “figure 1”, be used at both ends of the data exchange [9].

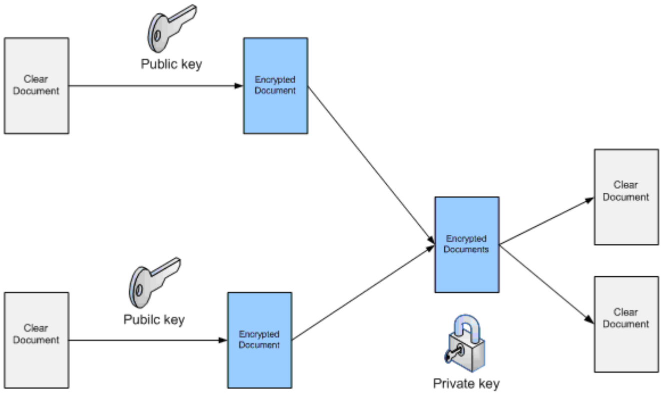


Figure 1: using public and private key for encryption

Asymmetric encryption classes usually use two separates keys for encryption and decryption. The device receiving the data uses a private key to decrypt data as it is received. Any remote device wanting to send encrypted data to the receiver must use a separate public key to encrypt the data before it is sent. The following figure represents our design and implementation of two world wide branches using VPN and IPSec technologies.

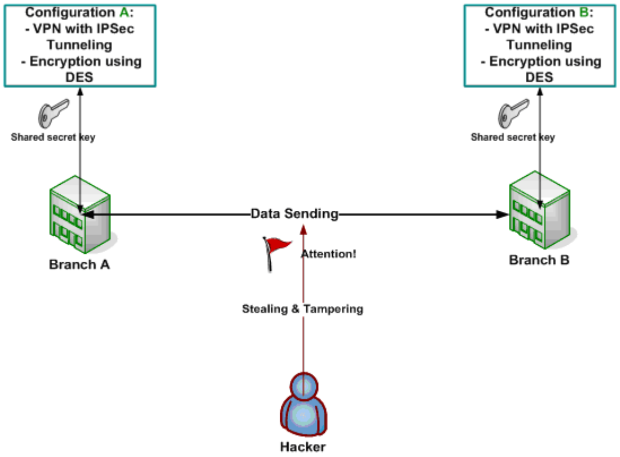


Figure 2: Proposed Security Design for WAN Topology

4. LAN PROTECTION

We have described previously our secure design for external network between companies. In this part we explain our secure design for the internal network of a branch and figure 3 below shows how our design of the local area network ‘LAN’ inside the office works step by step and organized in a way that allows secured and protected data communication to occur between users through security servers control inside the office. Therefore the system protection includes a special care for users, computers and information under main servers' control such the Active Directory 'AD', Windows Server Update Services 'WSUS', the Symantec Update, Windows Right Management Services 'WRMS', and SurfConrtol E-mail and Web Filtering 'SCEF'.

In order to make the LAN safe during sending and receiving messages, and during systems' job under administrator's control, there are many essential steps that keep the whole network process and users' access avoiding infections' threats, using specific protection's servers:

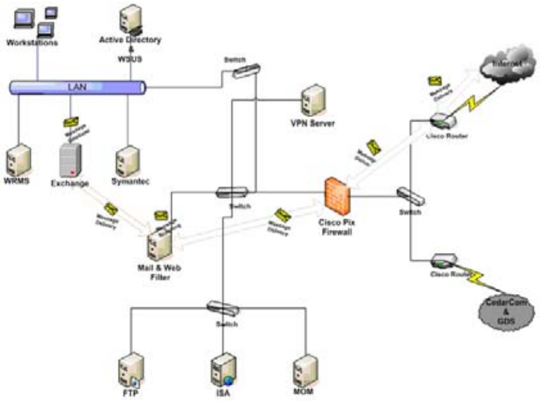


Figure 3: Proposed Security Design for LAN Topology

4.1 Active Directory

Active Directory 'AD' [1] server is a common repository for information about objects that reside on the network, such as users and groups, computers and printers, and applications and files. Administrators put all users in the office under control and give them permissions through the Active Directory 'AD' server's configuration which stores data about user, computers and network resources such as shared files, and printers, and lets only authorized users to access the AD.

The Group Policy Object 'GPO' is configured in the Active Directory and gives various permissions to all users depending on each user's job level. The GPO lets the administrator gives permission for users such as password policies to define its complexity and its length and age, and it can remove the run command from the start menu to restrict modifying the windows' system, also the most important policy is that it can restrict CD-ROM and floppy access to locally logged on, and to disable media source for any install to avoid having viruses problems and system's infection.

4.2 WSUS

To keep office systems protected and updated, the Windows Server Update Services 'WSUS' [5], which is configured in the Active Directory server, provides a capacity to download updates from Microsoft or from another WSUS server within user organization, and distributes these to its clients. WSUS provides a number of new features including targeting of patches to specific groups of machines, support for more products (e.g. Office), and improved reporting. WSUS is a service administrator run inside his organization – on one or more servers which he configures to serve software updates to one or more AU clients. Notice that AU client is an Automate Update Client which is a Windows Automatic Update software installed and running. The AU software contacts a Windows Update server and receives updates.

4.3 SurfControl E-mail and Web Filter

When the message gets inside the network, then the Pix Firewall scans and filters it against viruses. Therefore the SurfConftrol E-mail and Web Filter server [10] gets the message and starts analyzing and checking if it contains any spam or sex and adult words and any unsecured attachments, if the message is clean and clear, then the message continues on to reach the exchange server which provides a reliable messaging system that also protects against spam and viruses and finally the server distributes messages to all users in the office.

SurfControl E-mail Filter is a part of the SurfControl Enterprise Protection Suite, a unified threat management solution that also employs advanced Web and endpoint threat protection, to provide comprehensive protection against today's known, emerging and internal threats that increasingly exploit multiple threat points.

SurfControl Web Filter a best-in-class security solution that protects the enterprise against known, emerging, and costumer specific threats before they reach the network. It provides the strongest combination of protection, flexibility and scalability of any Web content security solution on the market. Also applying Web usage policies couldn't be easier.

4.4 Symantec Antivirus

The Symantec antivirus server [6] monitors, configures and updates each computer on the office's LAN network, also helping users to make their files better fortified against risks and viruses. Then the Symantec Antivirus main purpose is to protect files on your network and client computers from viruses and others risks, such as spyware and adware.

Each client on the network can be monitored, configured, and updated from a single computer by installing Symantec administrator tool that is called the Symantec System Center to verify which computers in the network are protected and working properly. The administrator can install and upgrade Symantec Antivirus clients and servers from the Symantec System Center.

4.5 WRMS

When a user needs to send a file to the other users internally then the Windows Rights Management Services 'WRMS' [7] server adds more security and protection to information. Depending on the importance of the file the user wants to send like customer data or financial reports, WRMS helps the user by letting him/her give specific permissions in which every recipient has specific jobs to do with that document, like read, save and print, or delete. So the sending file is protected by RMS. WRMS is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized user.

4.6 MOM

By delivering operational knowledge and subject expertise directly from the application developers, MOM [2] helps simplify identification of issues, reorganize the process for determining the root cause of the problem, and facilitates quick resolution to restore services and to prevent potential IT problems. So MOM allows user to monitor and generate reports on the total uptime of SQL Server and other service level exception. It manages all servers from centralize management (monitoring).

5. APPLICATION

This session discusses how these concepts come together into practical use in the banking system, with an applied focus on the network "communication" between the main office of the bank and its all branches. It also shows the actual practices of these concepts in the bank system, which are through the virtual private network "VPN" using a secure tunnel protocol and makes the virtual connection between user and company connected through remote access or site to site types within the external network, and the internal system protection using particular protected servers --- Active Directory 'AD', Windows Server Update Services 'WSUS', Symantec, and SurfControl for web and mail filter.

6. RESULT AND DISCUSSION

There are some special cases illustrate how the network can be protected and high level secured against hackers and viruses, actually during an email coming from the external to the internal network, and during the web browser access. Also keeping the inside company's system sheltered during sending messages between users, also avoid systems be infected by prohibit using device may include viruses such as CD, floppy or USB.

6.1 Case 1: Incoming E-mail

If the incoming e-mail includes any kind of threats that cause problems to the network and systems, then the Mail Filter server helps to protect and avoid system's infection by making a decision on whether or not an e-mail is infected or not. If an e-mail doesn't contain spam or/and viruses then the Exchange server permits the passage of this email to recipients. If infected, the e-mail gets isolated or discarded see figure 4.

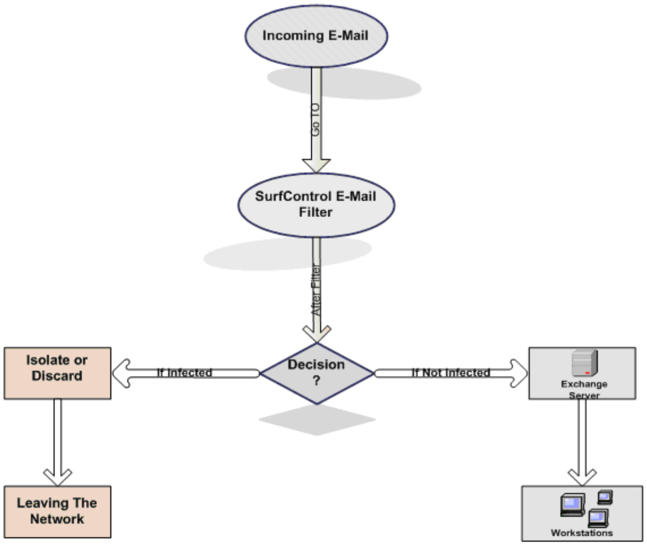


Figure 4: SurfControl Protection

6.2 Case 2: Spoofing Data

Data can be secured and protected against any outer theft and tampering, especially when data is being sent between branches, through the VPN connection using Internet security protocol 'IPSec' tunneling with the data encryption using data encryption standard 'DES'. Pre-shared keys are the simplest authentication method to implement and permit two branches communicate with each other in private, and their private key should exist the same and never given out "see figure 5.

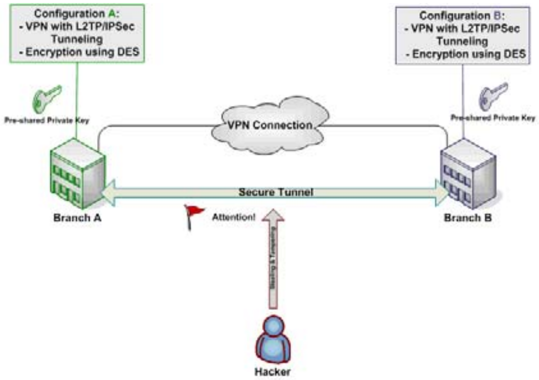


Figure 5: VPN with IPSec Encryption Technique

6.3 Case 3: Web Browsing

ISA server secures the network through firewall, and accelerates the web access during cashing "HTTP" which users request like HTTP protocol. At the same time, the web filter checks the web content with high level of protection against any unknown web browser that may cause specific threats before reaching the network 'see figure 6'. Then the Web Filter replies to HTTP request by allow or disallow depending on the web clearance.

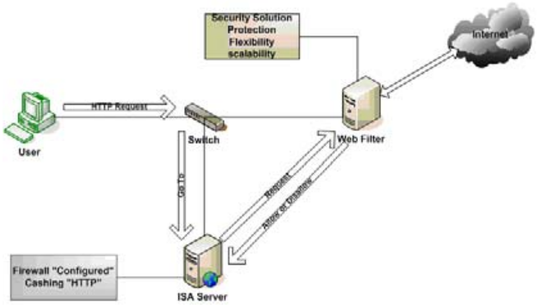


Figure 6: Web Filter Protection

6.4 Case 4: Active Directory

To avoid the infection and malfunction that viruses and hackers cause to systems in the internal network 'LAN', the Active Directory contains Group Policy Object 'GPO' which are controlled by the administrators who provide permissions to all users in the office. One of the most important permissions which is used against systems' threats is the policy of security options for 'disable the media source' for any install and access locally such as CD-ROM, Floppy and USB that may include viruses 'see figure 7'.

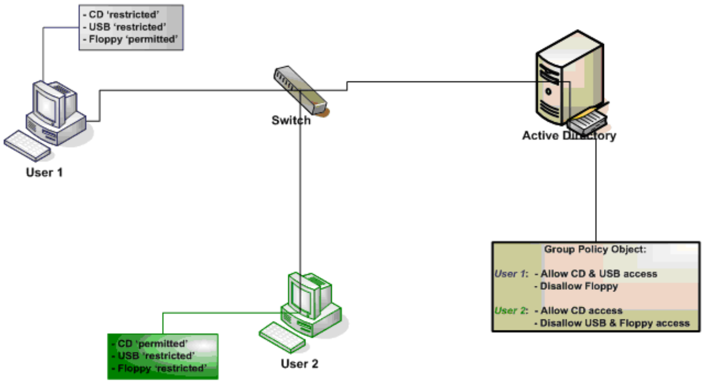


Figure 7: Active Directory Policy

6.5 Case 5: Encrypted File

The Windows Rights Management Services 'WRMS' helps protect information from unauthorized use in the network. Figure 8 shows that user 1 "the sender" sends a file internally to user 2 and user 3 by giving each one special limitation using the built in "Restrict Permission as". Then the user 1's computer will be configured for WRMS with contacting the WRMS server, and so the protected file contacts the WRMS server for license. Finally the RMS organizations help the sender to protect and prevent his file --- from intentionally getting into the wrong hand "user 4".

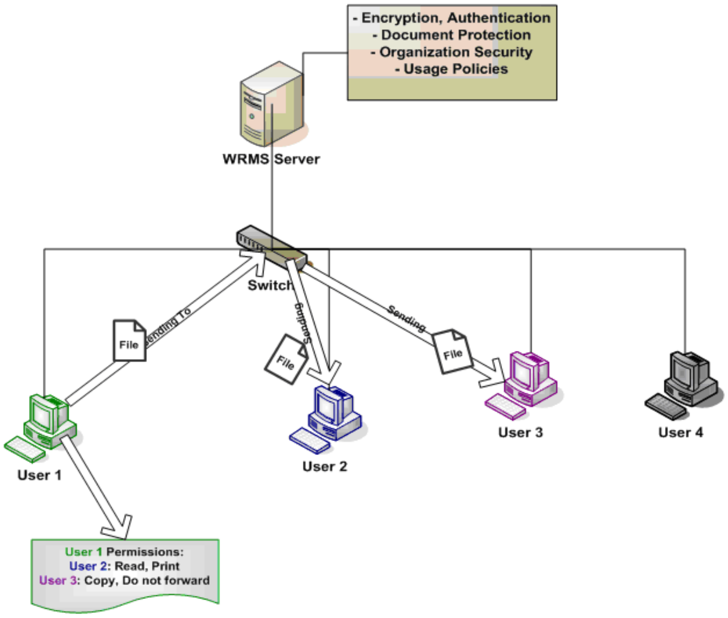


Figure 8: File Protected by WRMS Server

7. CONCLUSION

This article proposed a secure design for network and system in windows environment using the latest technology. The security of networks always faces new potential threats as hackers and viruses advance. The design shows how the network can be more secure by encrypting the sending data using internet protocol security between user and server. The purpose of network security is to provide availability, integrity, and confidentiality.

Thus, the main objective of VPN is to prevent outsiders (hackers) from interfering with messages sent among hosts in the network, and to protect the privacy and integrity of messages going through untrusted networks. The active directory manages all network resources such as servers, shared files, and printers, through authorization access resources. In addition to Active Directory, the main protection's servers such as WRMS, and WSUS, and Symantec make the internal network 'LAN' protected and secured against threats and viruses.

After applying our proposed design and these concepts to an enterprise with worldwide branches, they proved efficient and highly reliable as network security mechanism. Therefore, all the mechanisms thoroughly discussed in this project proved to work well together and provide the needed security in any professional setting.

REFRENCES

[1]. Allen R. and Alistair G, Active directory. O'Reilly 2003.

[2]. Fox C., Essential Microsoft Operations Manager. O'reily, 2006.

[3]. Munasinghe K. S. and Shahrestani S. A., “Evaluation of an IPSec VPN over a Wireless Infrastructure,” in Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC 2004), pp. 315-320, December 2004a.

[4]. Munasinghe K. S. and Shahrestani S. A., “Analysis of Multiple Virtual Private Network Tunnels over Wireless LANs,” in Proceedings of the 3rdInternational Business Information Management Conference (IBIMA 2004), pp. 206-211, December 2004b.

[5]. Piltzecker T., Williams D., Snedaker S., Todd C., Vigil K.. How to Cheat at Managing Windows Server Update Services. Syngress, 2006.

[6]. Shimonski Robert J., Configuring Symantec Antivirus: enterprise edition. Lavoisier, 2003.

[7]. Shinder D., How the Windows Rights Management Service can Enhance the Security of your Documents. Published: Sep 23, 2003 Updated: Apr 06, 2005 Section: Articles. Windows 2003 Security. www.windowsecurity.com

[8]. Stallings W., Cryptography and Network Security, 4/E Prentice Hall, 2006.

[9]. Stinson D., Cryptography Theory and Practice, Third Edition last modified January 19, CRC Press, 2006.

[10]. SurfControl Instant Message Filter, Administrator's Guide Version 4.5 printed June 30, 2004. www.surfcontrol.com

[11]. SÜHEYLA K ZIN, Performance parameters of wireless virtual private network. Master Thesis, Middle East University. 2006.