International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 5, Issue 6, June 2016)

Enhancing LAN Security Integrated Security Monitoring Tool

Monika[1], Savita Bisnoi[2]

[1]*M. Tech Scholar, CSE Dept, RIEM, Rohtak, MDU University Rohtak, India*
[2]*Associate Professor, CSE Dept, RIEM, Rohtak, MDU University Rohtak, India*

***Abstract: -* With the growth of networked systems all around us, it has become imperative for us to monitor their health so as to keep them secure from any external or internal threat. The internal threats being as important as well as the external threats. The users of the networked systems require secure systems and system resources that they can trust. The aim behind our approach is to provide an effective design in the hands of the systems and security administrator so as to help him maintain the required level of trust in his networked environment. The Integrated Security Monitoring Tool allows the administrator to monitor the file system, monitor the audit logs, bandwidth control, probe the system for vulnerabilities and maintain the integrity of important files in his environment.**

***Keyword:* LAN, Client-server, Integrated Security Monitoring Tool**

I. Introduction

Today, the internet provide home computer with the same networking power institutions outside the home have traditionally used. Figure 1.1 presents a simple Client-Server model. The basic features of a client's-server model are [1]:

1. The functions performed by a client and a server are complementary and can be implemented by a set of software modules, hardware components, or a combination thereof.
2. Each Clients/server relationship is established between two functional modules when one module (client) initiates a service request and the other (server) chooses to respond to the service request.
3. Information exchange between Clients and server is strictly through messages (i.e., no information is exchanged through global variables).
4. Messages exchanged are typically interactive. In other words, client and server model does not support an off-line process.

A Distributed Computing System (DCS) is a field of computer science that studies distributed system [2]. A distributed system is a software system in which components located on networked computers communicate and coordinate their action by passing messages.

Technically, the computers do not share main memory so that the information cannot be transferred through global variables.

II. Clients-Server Architectures

Client-server architecture is a network architecture in which each computer or process on the network is either or a server. Server is powerful computer or process dedicated to managing disk drive. Client is PCs or workstations on which user run applications. Clients and server typically communicate with each other by using one of the following paradigms.

Remote Procedure Call (RPC): In this paradigm, the client process invokes a remotely located procedure (a server process), the remote procedure executes and sends the response back to the client. The remote procedure can be simple (e.g., retrieve time of day) or complex (e.g., retrieve all customers from Delhi who have a good credit rating) [3]. Each request/response of an RPC is treated as a separate unit of work, thus each request must carry enough information needed by the server process. RPCs are supported widely at present.

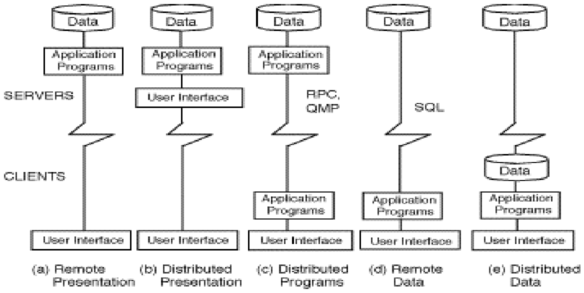


Figure 1 Traditional Clients/server Architectures

The remote data configuration at present is very popular for departmental applications and is heavily supported by numerous database vendors (as a matter of fact this configuration is used to represent typical two-tiered architectures that rely on remote SQL). Most data warehouses also use a remote data configuration because the data warehouse tools can reside on user workstations and issue remote SQL calls to the data warehouse.

III. Domain Name Service (DNS) Security

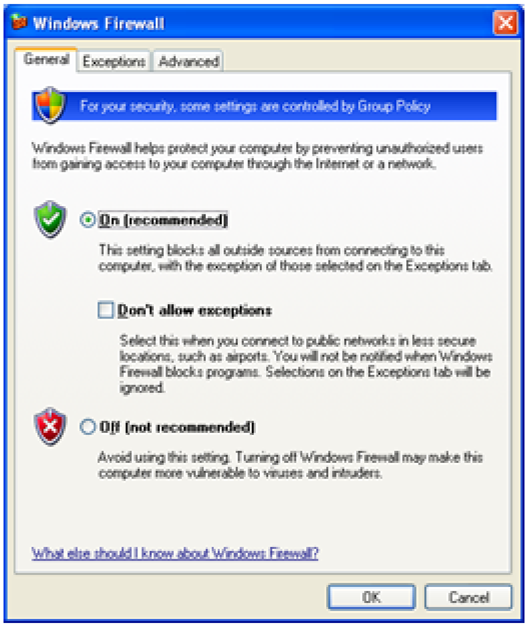
In the event of an unauthorized host becomes connected to your network, you can recognize it by its lack of a DNS entry. Many services can be configured to not accept connections from hosts that do not have valid DNS entries.

Descriptive hostnames are just as useful to attackers as they are to internal users. Host names such as ``firewall.mydomain.com" is obvious to an attacker, as is ``ns.mydomain.com". These are likely to be prime targets to an attacker [4]. A machine named ``fred.mydomain.com" likely indicates a normal user's PC, which is also least likely to have an updated security mechanism installed, making it also a prime target. These maps are then served over the network, allowing NIS client machines to get login, password, home directory and shell information (all the information in a standard /etc/passwd file), among other information.

IV. Windows Firewall

Windows XP Service Pack 2 (SP2) includes the Windows Firewall, a replacement for the feature previously known as the Internet Connection Firewall (ICF). Windows Firewall is a stateful host firewall that drops all unsolicited incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic).

The settings for ICF in Windows XP with SP1 and Windows XP with no service packs installed onsist of the Protect my computer and network by limiting or preventing access to this computer from the Internet check box on the Advanced tab of the properties of a connection, and a Settings button from which we can configure excepted traffic, logging settings, and excepted ICMP traffic.



For your security, some settings are controlled by Group Policy

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?

Fig 2 Firewall dialog box

When we configure Windows Firewall in an organization network using Group Policy, depending on the Group Policy settings, some of the local Windows Firewall configuration options might be grayed out and unavailable, even for local administrators.

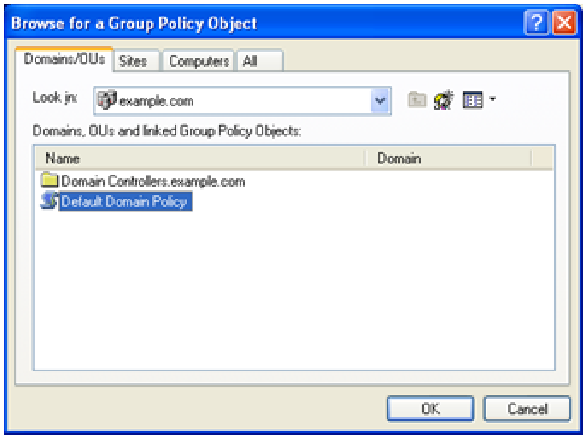
V. Deploying Windows Firewall

This method requires the use of Active Directory with either Windows 2000 or Windows Server 2003 domain controllers [5]. Group Policy updates are requested by the domain member computer, and are therefore solicited traffic that is not dropped when Windows Firewall is enabled.

Step 1: Updating Wer Group Policy Objects with the New Windows Firewall Settings

To update wer Group Policy objects with the new Windows Firewall settings using the Group Policy snap-in (provided with Windows XP), do the following:

1. Install Windows XP SP2 on a computer that is a member of the domain that contains the computer accounts of the other computers running Windows XP on which we plan to install Windows XP SP2.
2. Restart the computer and log on to the Windows XP with SP2-based computer as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
3. From the Windows XP desktop, click Start, click Run, type mmc, and then click OK.
4. On the File menu, click Add/Remove Snap-in.
5. On the Standalone tab, click Add.
6. In the Available Standalone Snap-ins list, click Group Policy Object Editor, and then click Add.
7. In the Select Group Policy Object dialog box, click Browse.
8. In the Browse for a Group Policy Object, click the Group Policy object that we want to update with the new Windows Firewall settings. An example is shown in the following figure.



Browse for a Group Policy Object

Domains/OUs | Sites | Computers | All

Look in: example.com

Domains, OUs and linked Group Policy Objects:

Name	Domain
Domain Controllers.example.com	
Default Domain Policy	

OK | Cancel

Step 2: Specifying Windows Firewall Settings for Wer Group Policy Objects

After a Group Policy object has been updated, it can be configured for Windows Firewall settings that are appropriate for Windows Firewall and the use of management, server, listener, or peer applications and services that are being run on wer computers running Windows XP with SP2.

There are two sets of Windows Firewall settings to configure [6]:

- The domain profile settings that are used by the computers when they are connected to a network that contains domain controllers for the domain of which the computer is a member.
- The standard profile settings that are used by the computers when they are connected to a network that does not contain domain controllers for the domain of which the computer is a member.

Drawbacks

The major drawback of Windows XP firewall is that it is client oriented and it lack client server building approach, and also its not full secure if we look up the single system policy then it could be used but it is not fully accepted by users.

VI. Implementation

In the Squid first to define which port a client need to open and rest to closed to avoid any overhead of squid server. List of port defined in safe and dangerous can be change as per user's request. The administrator will check it update the port by auditing the log analysis.

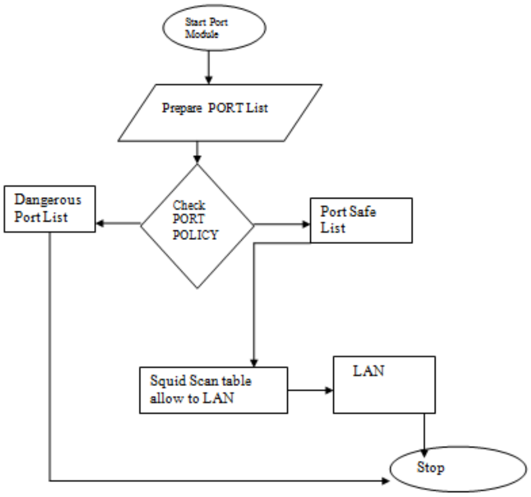


Fig.3 Flow Chart for Port Management

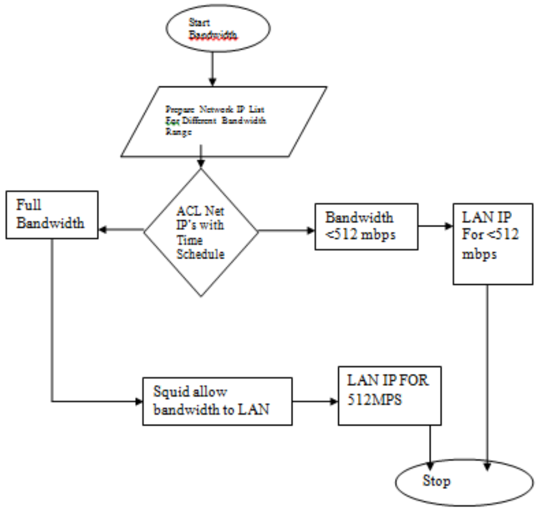

Start
Bandwidth
Prepare Network IP List For Different Bandwidth Range
ACL Net IP's with Time Schedule
Full Bandwidth
Bandwidth <512 mbps
LAN IP For <512 mbps
Squid allow bandwidth to LAN
LAN IP FOR 512MPS
Stop

Fig. 4 Flow Chart for Bandwidth Management

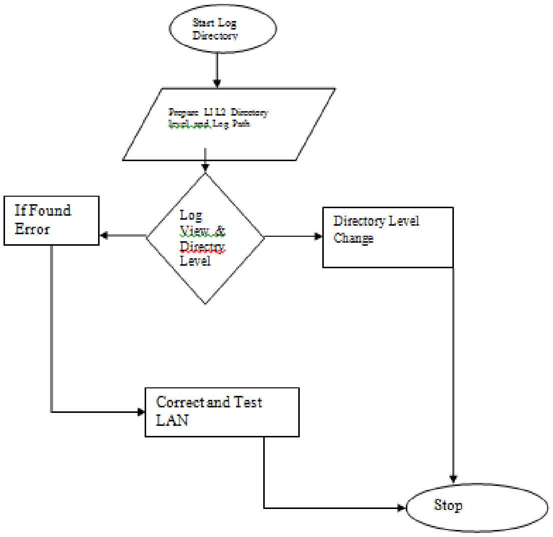


Fig. 5 Flow Chart for LOG and Directory Management

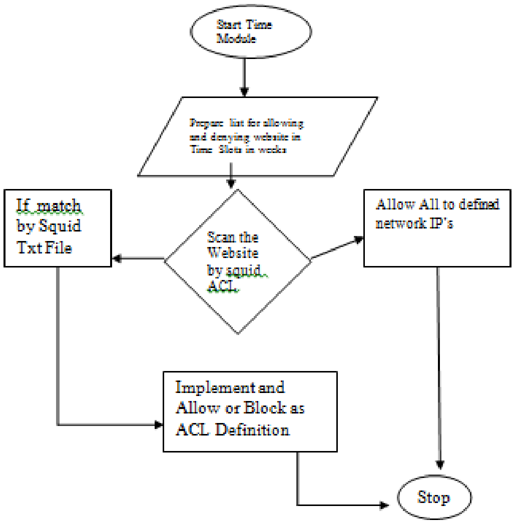

Start Time Module
Prepare list for allowing and denying website in Time Slots in weeks
Scan the Website by squid ACL
If match by Squid Txt File
Allow All to defined network IP's
Implement and Allow or Block as ACL Definition
Stop

Fig 6 Flow Chart for Time Management

VII. CONCLUSION

This paper described the design, implementation of the squid prosy server. The Squid Proxy server serves as better internet and firewall services for cooperative organizations having multiple uplinks. It can be easily deployed with the windows environments. It is scalable with different bandwidth monitoring systems. Further it keeps room for individual organizations to set their own policies giving first priority to the local users while sharing excess bandwidth with the neighbor proxies.

REFERENCES

[1] Saini, "Squid Proxy Server Beginners Guide" Packt Publishing, Open Source Community, 2011

[2] F. Schmidt, The SCSI Bus & IDE Interface, Protocols, Applications & Programming. Addison- Wesley, 1998

[3] M. McKusick, W. Joy, S. Leffler, R. Fabry, "A Fast File System for Unix", ACM Trans. On Comp. Sys. 2(3), pp. 181-197, Aug. 1984.

[4] Brian White, Wee Teck Ng, Bruce K. Hillyer "Performance Comparison of IDE and SCSI Disks" http://citeseerx.ist.psu.edu.

[5] Jia Wang, "A Survey of Web Caching Schemes for the Internet," ACM Computer Communication Review, 29(5):36--46, October 1999.

[6] The Automatization of Information Security of Local Calculation Network with the Open Access to Internet on FreeBSD Base" IEEE Paper CADSM"2009, 24-28 February, 2009, by Writer "Andrian Piskozub, Dmytro Levytskyy, Igor Rudyk, Larisa Rakobovchuk".

[7] https://saravanesh.files.wordpress.com/2010/06/introduction-to-client1.doc

[8] https://technet.microsoft.com/en-us/library/cc507834.aspx

[9] http://www.linuxsecurity.com/docs/SecurityAdminGuide/SecurityAdminGuide-3.html