Design and Implementation of a Network Security Model for Cooperative Network

Salah Alabady
Computer Engineering Department, University of Mosul, Iraq

Abstract: *In this paper a design and implementation of a network security model was presented, using routers and firewall. Also this paper was conducted the network security weakness in router and firewall network devices, type of threats and responses to those threats, and the method to prevent the attacks and hackers to access the network. Also this paper provides a checklist to use in evaluating whether a network is adhering to best practices in network security and data confidentiality. The main aim of this research is to protect the network from vulnerabilities, threats, attacks, configuration weaknesses and security policy weaknesses.*

Keywords- *Network security, network management, threats, security policy*

Received December 17, 2008; Accepted March 2 2009

1. Introduction

Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues [1]. The evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly exercised attacks causing damage or committing theft. The Internet continues to grow exponentially. As personal, government and business-critical applications become more prevalent on the Internet, there are many immediate benefits. However, these network-based applications and services can pose security risks to individuals as well as to the information resources of companies and government. In many cases, the rush to get connected comes at the expense of adequate network security. Information is an asset that must be protected [2].

Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset. Network security is the process by which digital information assets are protected, the goals of security are to protect confidentiality, maintain integrity, and assure availability. With this in mind, it is imperative that all networks be protected from threats and vulnerabilities in order for a business to achieve its fullest potential. Typically, these threats are persistent due to vulnerabilities, which can arise from mis-configured hardware or software, poor network design, inherent technology weaknesses, or end-user carelessness. A router is similar to many computers in that it has many services enabled by default. Many of these services are unnecessary and may be used by an attacker for information gathering or for exploitation. All unnecessary services should be disabled in the router configuration to prevent the attacker from using it to damage the network or to stealing the important information, or network devices configuration. In this paper a review of attacks on routers, and how can prevent, or mitigating it will be described. Routers and firewall are very critical parts of network operations and network security. Careful management and diligent audit of router and firewall operations, can reduce network downtime, improve security, prevent the attacks and hackers, network threats decrease, and aid in the analysis of suspected security breaches.

2. Network Security and Protection

Security has one purpose, to protect assets. With the advent of personal computers, LANs, and the wide-open world of the Internet, the networks of today are more open. As e-business and Internet applications continue to grow, finding the balance between being isolated and being open will be critical. With the increased number of LANs and personal computers, the Internet began to create untold numbers of security risks. Firewall devices, which are software or hardware that enforce an access control policy between two or more networks, were introduced. This technology gave businesses a balance between security and simple outbound access to the Internet, which was mostly used, for e-mail and Web surfing.

Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers [3, 4]. Network security refers to all hardware and software functions, characteristics, features, operational procedures, accountability measures, access controls, administrative and management policy required to provide an acceptable level of protection for hardware, software, and information in a network. Network security, in order for it to be successful in preventing information loss,

must follow three fundamental precepts. First, a secure network must have integrity such that all of the information stored therein is always correct and protected against fortuitous data corruption as well as willful alterations. Next, to secure a network there must be confidentiality, or the ability to share information on the network with only those people for whom the viewing is intended. Finally, network security requires availability of information to its necessary recipients at the predetermined times without exception. The three principles that network security must adhere to evolved from years of practice and experimentation that make up network history.

Real-world security includes prevention, detection, and response. If the prevention mechanisms were perfect, you wouldn't need detection and response. But no prevention mechanism is perfect. Without detection and response, the prevention mechanisms only have limited value. Detection and response are not only more cost effective but also more effective than piling on more prevention. On the Internet, this translates to monitoring. In Network Protection, there are fortunately many preventative techniques to properly secure network against threats. The first method of protection is to address the actual physical layer of the network to assure that it is properly equipped. Next, three network administrative guidelines should be adhered to [5, 6].

Additionally, firewalls and encryption should be incorporated into a network to heighten its security. Finally, several other passwords, variations of capital and small letters further increase the strength of a password. Proper authentication is an integral part of the administrative step in securing a network. Firewalls are yet another measure used in increasing the level of security in a network. A firewall is in essence a portal through which information enters and exits.

On one side of the portal is the internal network that must remain secure, and on the other is the information needed from the outside world combined with the undesirable threats of external networks. Three of the major types of firewalls, listed in order of increasing quality and price, are packet-filtering routers, application-level gateways, and circuit-level gateways. Although it is not the best available firewall, a positive step in increasing network security is the use of packet-filtering routers. A packet filtering router allows the network to determine which connections can pass through the router into the local area network and which connections will be denied. The application-level gateway is designed specifically as a firewall that authenticates the user for individual applications. Its primary function is to identify and validate the user and then provide access to specific applications such as E-Mail or file browsers depending on which one the user is requesting. Finally, a circuit-level gateway performs all of the packet-filtering that a router does and a bit more. The primary enhancement is the use of identification and authentication before an insider can access your in-house network.

3. Weaknesses, Threats and Attacks on Router

When discussing network security, three common terms used are vulnerability, threat, and attack. Vulnerability is a weakness, which is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves. There are three primary vulnerabilities or weaknesses: [7, 8, and 9]

1. Technology weaknesses
2. Configuration weaknesses
3. Security policy weaknesses

Technological Weaknesses: Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Configuration Weaknesses: Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate. Some common configuration weaknesses are listed in Table 1. [10, 11]

Security Policy Weaknesses: Security policy weaknesses can create unforeseen security threats. The network may pose security risks to the network if users do not follow the security policy. Some common Security Policy Weaknesses are listed in table 2. Threats are the people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses. Finally, the threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. In this paper we will discuss the two primary classes of threats to network security, there are internal threats and external threats. Internal threats to a network are a major source of strain on the level of security attained by that network.[10] These threats generally stem from either disgruntled or unethical employees.

External threats to network security, generally referred to as hackers, can be equally and sometimes more dangerous than internal threats. To obtain entry into a network or view sensitive information, hackers must use some tools such as: 1- password sniffers, 2- IP snooping, 3- E-Mail attacks. Password sniffers actually work with the execution of a packet sniffer that monitors traffic on a network passing through the machine on which the sniffer resides. The sniffer acquires the password and log-on name used when the source machine attempts to connect to other machines and saves this information in a separate file later

obtained by the hacker. IP spoofing involves the capturing of the information in an Information Packet (IP) to obtain the necessary address name of a workstation that has a trusted relationship with yet another workstation. In doing so, a hacker can then act as one of the workstation and use the trusted relationship to gain entry into the other workstation where any number of actions can be performed. Finally, E-Mail is extremely vulnerable and quite susceptible to a number of different attacks.

Regardless of the method used to gain entry onto a network or view communications therein, hackers can truly jeopardize a network, security and potentially do severe damage to the data and systems within. Additional forms of malicious software, such as Trojan horses, worms, and logic bombs exist as threats to network security. Table 3, shows identify the potential "threats" to each of these elements. The general threats on router or firewall network device include but are not limited to: unauthorized access, session hijacking, rerouting, masquerading, denial of service (DoS), eavesdropping, and information theft. While Attack techniques include: password guessing, routing protocol attacks, simple network management protocol (SNMP) attacks, IP fragmentation attacks – to bypass filtering, redirect (address) attacks, and circular redirect – for denial of service. Here we will explain the action of some attacks.

1. The session replay attacks use a sequence of packets or application commands that can be recorded, possibly manipulated, and then replayed to cause an unauthorized action or gain access.
2. Rerouting attacks can include manipulating router updates to cause traffic to flow to unauthorized destinations. These kinds of attacks are sometimes called "route injection" attacks.
3. Masquerade attacks, these attacks occur when an attacker manipulates IP packets to falsify IP addresses. Masquerades can be used to gain unauthorized access or to inject bogus data into a network.
4. Session hijacking attack: this attack may be occur if an attacker can insert falsified IP packets after session establishment via IP spoofing, sequence number prediction and alteration, or other methods.
5. Land attack, the land attack involves sending a packet to the router with the same IP address in the source and destination address fields, and with the same port number in the source port and destination port fields. This attack may cause denial of service or degrade the performance of the router.
6. TCP SYN Attack, the TCP SYN attack involves transmitting a volume of connections that cannot be completed at the destination. This attack causes the connection queues to fill up, thereby denying service to legitimate TCP users.
7. Smurf Attack**,** this attack involves sending a large amount of ICMP echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet. If a router is positioned to forward broadcast requests to other routers on the protected network, then the router should be configured to prevent this forwarding from occurring. This blocking can be achieved by denying any packets destined for broadcast addresses.
8. Distributed Denial of Service (DDoS) Attacks, several high-profile DDoS attacks have been observed on the Internet. While routers and firewall, cannot prevent DDoS attacks in general, it is usually sound security practice to discourage the activities of specific DDoS agents by adding access list rules that block their particular ports. But some of these rules may also impose a slight impact on normal users, because they block high-numbered ports that legitimate network clients may randomly select. Therefore, you may choose to apply these rules only when an attack has been detected. Otherwise, these rules would normally be applied to traffic in both directions between an internal or trusted network and an untrusted network examples of denial of service attacks are (Ping of death, SYN flood attack, Packet fragmentation and reassembly, E-mail bombs, CPU hogging, Malicious applets, Misconfiguring routers, The chargen attack, Out-of-band attacks such as WinNuke, Land.c, Teardrop.c,, Targa.c, Masquerade/IP Spoofing).

4. Router and Firewall Security Policy

Routers perform many different jobs in modern networks, forwards traffic between two or more local networks within an organization or enterprise routes. Interior routers may impose some restrictions on the traffic they forward between networks. Forwards traffic between different enterprises (sometimes called different 'autonomous systems'). The traffic between the different networks that make up the Internet is directed by backbone routers.

The level of trust between the networks connected by a backbone router is usually very low. Typically, backbone routers are designed and configured to forward traffic as quickly as possible, without imposing any restrictions on it. The primary security goals for a backbone router is to ensure that the management and operation of the router are conducted only by authorized parties, and to protect the integrity of the routing information it uses to forward traffic. Backbone routers typically employ Exterior Gateway Protocols to manage routes [5].

Configuring backbone routers is a very specialized task. The border router forwards traffic between an enterprise and exterior networks. The key aspect of a border router is that it forms part of the boundary between the trusted internal networks of an enterprise,

and untrusted external networks (e.g. the Internet). It can help to secure the perimeter of an enterprise network by enforcing restrictions on the traffic that it controls. A border router may employ routing protocols, or it may depend entirely on static routes.

Security policy is the definition of security function against a network intrusion. Security engine provides security functions of a packet filtering, an authentication, an access control, an intrusion analysis and an audit trail in the kernel region of router [10, 12]. Router is a key component of the Internet, and an important part of networks that controls a data packet flow in a network and determines an optimal path to reach a destination, and their security is a vital part of the overall security for the networks they serve. An error of the router or an attack against the router can damage an entire network. Since the router is connected to at least two networks and manages network traffic, the security is necessary to control of an unauthorized router access and an illegal network intrusion. Secure router technology has security functions, such as intrusion detection, IPsec and access control, are applied to legacy router for secure networking. A router may be responsible for filtering traffic, allowing some packets to pass through and rejecting others [13]. Filtering can be a very important function of routers; it allows them to help protect computers and other network components. It is also possible that at the destination end a router may have to break large packets up to accommodate the size limits of the destination LAN. Modern routers do not only perform relaying functions, but also filtering, separation, encryption and monitoring of data streams. Furthermore, they provide various management interfaces for configuration, (remote) maintenance, and monitoring. All these functions potentially affect the availability, integrity, and confidentiality of data connections, thus making routers highly security-critical network components. However, configuring a router is a difficult and error prone task.

A firewall can protect a network from external attacks by examining all packets of a message attempting to pass through the network and rejecting the packets that do not meet the security restrictions. However, it does not protect the data as it is transmitted from one network to another. Data transmitted from one network to another via the Internet is susceptible to access at many points between the source and destination. The secure socket layer (SSL) is one means of providing secure communications between points connected via the Internet.

Routers and firewall support a large number of network services at layers 2, 3, 4, and 7 [14]. Some of these services are application layer protocols that allow users and host processes to connect to the router, firewall and others network devices. Others are automatic processes and settings intended to support legacy or specialized configurations, which are detrimental to security. Some of these services can be restricted or disabled to improve security without degrading the operational use of the router and the network performance. Also attacks and hackers can utilize these services to find the weakness point in the network. General security practice for routers and firewall should be to support only traffic and protocols a network needs. Examples for these services are:

1. CDP, the Cisco Discovery Protocol is a proprietary protocol that Cisco routers use to identify each other on a LAN segment. It is useful only in specialized situations, and is considered deleterious to security.
2. TCP and UDP Small Servers, the TCP and UDP protocol standards include a recommended list of simple services that hosts should provide. In virtually all cases, it is not necessary for routers to support these services, and they should be disabled.
3. Finger Server, the IOS finger server supports the Unix 'finger' protocol, which is used for querying a host about its logged in users.
4. HTTP Server, most router and firewall support web-based remote administration using the HTTP protocol. While the web access features are fairly rudimentary on most routers, they are a viable mechanism for monitoring, configuring, and attacking a router. If web-based remote administration is not needed, then it should be disabled as shown below. Web-based remote administration is useful primarily when intervening routers or firewalls prevent use of Telnet for that purpose. However, it is important to note that both Telnet and web-based remote administration reveal critical passwords in the clear. Therefore, web-based remote administration should be avoided.
5. Bootp Server**,** Bootp is a datagram protocol that is used by some hosts to load their operating system over the network. Cisco routers are capable of acting as bootp servers, primarily for other Cisco hardware. This facility is intended to support a deployment strategy where one Cisco router acts as the central repository of IOS software for a collection of such routers. In practice, bootp is very rarely used, and offers an attacker the ability to download a copy of a router's IOS software.
6. Configuration Auto-Loading**,** some routers such as Cisco routers and Linksys routers, are capable of loading their startup configuration from local memory or from the network. Loading from the network is not secure, and should be considered.
7. IP source routing, source routing is a feature of IP whereby individual packets can specify routes. This feature is used in several kinds of attacks. Cisco routers normally accept and process source routes. Unless a network depends on source routing, it should be disabled on all the net's routers.

8. Proxy ARP, network hosts use the Address Resolution Protocol (ARP) to translate network addresses into media addresses. A router can act as intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments. This service is called proxy ARP. Because it breaks the LAN security perimeter, effectively extending a LAN at layer 2 across multiple segments, proxy ARP should be used only between two LAN segments at the same trust level, and only when absolutely necessary to support legacy network architectures.
9. IP Directed Broadcast, directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. This technique was used in some old denial of- service attacks. Therefore it must disable this function.
10. IP Unreachable, Redirects, and Mask Replies: the Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Cisco routers automatically send ICMP messages under a wide variety of conditions. Three ICMP messages are commonly used by attackers for network mapping and diagnosis: 'Host unreachable', 'Redirect', and 'Mask Reply'. Automatic generation of these messages it is important to be disabled on all interfaces, especially interfaces that are connected to untrusted networks.
11. SNMP Services, the Simple Network Management Protocol (SNMP) is the standard Internet protocol for automated remote monitoring and administration. There are several different versions of SNMP, with different security properties. If a network has a deployed SNMP infrastructure in place for administration, then all routers on that network should be configured to securely participate in it. As example a Cisco router can be configured to act as a client for SNMP. When SNMP service is enabled on a router, network management tools can use it to gather information about the router configuration, route table, traffic load, and more. In the absence of a deployed SNMP scheme, all SNMP facilities on all routers should be disabled using these steps:

1. Erase all existing community strings.
2. Disable SNMP system shutdown and trap features.
3. Disable SNMP system processing.

5. Creating and Implementing a Security Policy.

Turning off a network service on the router or firewall itself does not prevent it from supporting a network where that protocol is employed. For example, a router may support a network where the bootp protocol is employed, but some other host is acting as the bootp server. In this case, the router's bootp server should be disabled. Turning off an automatic network feature usually prevents a certain kind of network traffic from being processed by the router or prevents it from traversing the router. For example, IP source routing is a little-used feature of IP that can be utilized in network attacks. Unless it is required for the network to operate, IP source routing should be disabled. Figure (1) shows the structure of the suggested network security model.

In this section of paper we will mention some setups, that must be considered to applied in configuration mode for the router and firewall in the network to achieve the best security and to prevent several kinds of attacks, and to protect against the mentioned types of vulnerabilities, threats and attacks on the network. The philosophy of the suggested security solutions is based on using multiple tips of protection and it could be explained as followed:

1. The first is to build physical security by creating security policy, considered who is authorized to install, de-install, move both the router and firewall, and to change the physical configuration or physical connections to the router or firewall. Designates who is authorized to log in directly to the router via the console or other direct access port connections. Also, define the password policy for user/login passwords, and for administrative or privilege passwords.
2. Designates who is authorized to log in to the router remotely (Telnet, SSH) and limits on use of automated remote management and monitoring facilities (e.g. SNMP).
3. Configure and enable secret password for console, auxiliary port, and VTY ports on each network device. This will prevent unauthorized from access direct to any network devices.
4. Encrypting all passwords by using service password-encryption command to prevent the attacks and hacker from recovery the secret password. Also it is important to disable the service password-recovery, to deny the attack from recover the password or to erase the password when reboot the router.
5. Set the minimum character length for all routers, firewall passwords. This provides enhanced security access to the router by allowing you to specify a minimum password length.
6. Controlling the virtual terminal lines (VTYs), any VTY should be configured to accept connections only with the protocols actually needed. Also the last VTY might be restricted to accept connections only from a single, specific administrative workstation, whereas the other VTYs might accept connections from any address in a corporate

network. Another useful tactic is to configure VTY timeouts using the exec-timeout command.

7. Enabling Transmission Control Protocol (TCP) keep lives on incoming connections, this can help guard against both malicious attacks and orphaned sessions caused by remote system crashes.
8. Disabling all non-IP-based remote access protocols, and using SSH, SSL, or IP Security (IPSec) encryption for all remote connections to the router instead of TELNET, this can provide complete VTYs protection. Remote administration is inherently dangerous because anyone with a network sniffer on the right LAN segment can acquire the router passwords and would then be able to take control of the router.
9. Disable unneeded features and services on route such as: CDP, http server, bootp server, IP directed broadcasts, TCP small services, UDP small services, IP source routing.
10. Disable (shut down) unused interfaces on all routers and firewall, this helps discourage unauthorized use of extra interfaces, and enforces the need for router administration privileges when adding new network connections to a router.
11. Set up usernames and passwords for all administrators. Or one can use AAA user access control, AAA will give more control and better audit. AAA is the acronym for authentication, authorization, and accounting.
12. Applied access control lists, to filtering the malicious traffic packets, and to rate limiting, this filtering can usually be done based on two criteria:

    - The source and destination IP addresses of the traffic.
    - The type of traffic.

    The access control lists can reject all traffic from the internal networks that bears a source IP address which does not belong to the internal networks, reject all traffic from the external networks that bears a source address belonging to the internal networks and reject all traffic with a source or destination address belonging to any reserved, unroutable, or illegal address range.
13. It is important to allow only local access because during remote access, all telnet passwords or SNMP community strings are sent in the clear to the router. If an attacker can collect network traffic during remote access then he can capture passwords or community strings. However, there are some options if remote access is required. Establish a dedicated management network. The management network should include only identified administration hosts and a spare interface on each router. Another method is to encrypt all traffic between the administrator's computer and the router, by setting up IPSec encryption or SSH encryption. SSH also prevents session hijacking and many other kinds of network attacks.
14. No local user accounts are configured on the router. Routers must use Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial In User service (RADIUS) protocols for all user authentications.
15. Configure local AAA (Authentication Authorization Account) on router and firewall, the local data base, and Authentication using AAA, additionally configure Authentication proxy. This is Cisco's new access control facility for controlling access, privileges, and logging of user activities on a router. Authentication is the mechanism for identifying users before allowing access to a network component. Authorization is the method used to describe what a user has the right to do once he has authenticated to the router. Accounting is the component that allows for logging and tracking of user and traffic activities on the router which can be used later for resource tracking or trouble shooting.
16. Using NAT, a router can hide the structure of the trusted network, by transparently translating all IP addresses and coalescing distinct IP addresses into a single one.
17. Using Cisco IOS firewall Intrusion Detection System (IDS) is a real-time IDS designed to enhance border router security by detecting, reporting, and terminating unauthorized activity. This facility is available in IOS releases for many, but not all, Cisco routers. A unique benefit of implementing an IDS on a router, especially a border router, is that all network traffic flows through it and may be examined.
18. A poor router filtering configuration can reduce the overall security of an network, expose internal network components to scans and attacks, and make it easier for attackers to avoid detection. Careful router configuration can help prevent a (compromised) site from being used as part of a distributed denial of service (DDoS) attack, by blocking spoofed source addresses. DDoS attacks use a number of compromised sites to flood a target site with sufficient traffic or service requests to render it useless to legitimate users.
19. Apply port security on the switch to mitigate CAM table overflow attacks. once can apply port security in three ways: Static secure MAC addresses, Dynamic secure MAC addresses and Sticky secure MAC addresses. The type of action taken when a port security violation occurs falls into the following three categories: Protect, Restrict, Shutdown.
20. Using PacketShaper, it is a traffic management appliance that monitors and controls IP network traffic going over wide-area networks (WAN) links. It keeps critical traffic moving at an appropriate pace through bandwidth bottlenecks and prevents

any single type of traffic from monopolizing the link. Also PacketShaper identifies and analyzes inbound and outbound WAN traffic up to and including the OSI Application Layer (Layer 7). PacketShaper manages WAN link utilization and throughput based on the bandwidth reservations and policies applied to the identified traffic classes. In addition,PacketShaper provides a comprehensive view of the applications that are running on your network. And by using PacketShaper, once can:

- Determine what is running on the network and traversing the link
- Find out how each application is performing
- . Determine how much bandwidth each application is using
- Guarantee bandwidth to mission-critical applications and keep non-critical applications from overwhelming the link.

6. Test Bed and Performance Testing

In order to test the security and performance of the suggested network model, a test bed was build and establish as shown in Figure (2). The test bed is consisted from the two Cisco router 2811, Cisco firewall (PIX) 516E , Cisco switch 2960, AAA server with TACACS+ protocol and two workstation work as real attacker and hacker.

The following procedures were taken to examine the network operation to test the network security robustness against different types of attacks. Also some scanning tools are used to simulate real network attacks and intrusions on the target system.

1. Ethereal program (network traffic capture and analysis tool) was used to simulate real reconnaissance network attacks on the target network. This program used to see what is on the network (as the hacker does before his attack), also this program is an effective "sniffer". Try to obtain the password for network devices and other information in the network such as routing table or CAM table, but because encrypting all passwords by using service password-encryption command, and disable the CDP on the routers, and using SSH, SSL, IP Security (IPSec) encryption for all remote connections instead of TELNET, the attacks and hacker prevent from recovery the secret password and theft the information.
2. Super Scanner program used to simulate a real access attacks to find which the IP address is active or which port is active and open in the network, the purpose to obtain the network IP address of a workstation or IP address of a network device, port scanner to discover which port is used and open. This action was detected and prevented by the firewall, techniques security and the accesses control list that applied on the router and firewall.
3. Nmap program which is used to scan for open TCP and UDP ports on a router and firewall interface ports. The attack and hacker use a port scanner tools to estimate the network map then he can find how the network structured and what software is running on it. This action was prevented and denies by the disable unneeded features and services on route and firewall such as: CDP, http server, bootp server, IP directed broadcasts, TCP small services, UDP small services.
4. Nessus program, this program used to search the vulnerabilities in the network. This action was prevented by disable (shut down) unused interfaces on all routers and firewall, Disable unneeded features and services on route such as: CDP, http server, bootp server, IP directed broadcasts, TCP small services, UDP small services, IP source routing. Also the network address translation (NAT) is hides information about the network by making it seem that all outgoing traffic originates from the firewall rather than the network.
5. Trying to use the TELNET service to access to the router and firewall. This action was prevented because disabling all non-IP-based remote access protocols, and using SSH, SSL, IP Security (IPSec) encryption for all remote connections, there are secret password for console, auxiliary port, and VTY ports on each network device, also the routers use TACACS+ protocols for all user authentications.
6. Used Dsniff programs (a collection of tools to do ARP spoofing) to simulate a DoS attacks , this action was stopped and prevented by applied access control lists on router and firewall to filtering the malicious traffic packets, and reject all traffic from the internal networks that bears a source IP address which does not belong to the internal networks.
7. Unauthorized attempts to access to the network resources and devices, this action was detected and prevented by AAA server and firewall network, because the firewall and AAA server and screen both incoming and outgoing traffic in the network.
8. Kiwi Syslog program, which is used to capture and preserve log messages from Cisco routers and many other network devices, this action prevented by Disabling some protocols on the network devices, to prevent attacks and hackers used it, but without affects on the performance of the networks, such as finger protocol requests, Network Time Protocol, Cisco Discovery Protocol (when used Cisco network device), Internet Control Message Protocol (ICMP), multicast route caching Protocol , proxy ARP Protocol.
9. Used Macof tools program to do MAC spoofing and **C**AM table overflow attacks. This action was prevented by apply port security on the switch in three ways: static secure MAC addresses, dynamic

secure MAC addresses and sticky secure MAC addresses.

After doing the previous several tests, the proposed configuration showed a very efficient security performance keeping a high performance of the network speed and services. Also from the test results, we can protect the network from various types of attacks such as Access attacks, Password Attacks, Denial of service attacks and make it easier for attackers to avoid detection.

7. Conclusion

This paper deals with and discusses the security weakness in router and firewall configuration system and risks when connected to the Internet .Also this paper presented the tips and recommendations to achieve a best security and to protect the network from vulnerabilities, threats, and attacks by applying the security configurations on router and firewall. Also one can use this suggested security policy as a checklist to use in evaluating whether a unit is adhering to best practices in computer security and data confidentiality. This work appears the firewall provides additional access control over connections and network traffic and perform user authentication. Using a firewall and a router together can offer better security than either one alone. A poor router filtering configuration can reduce the overall security of a network, expose internal network components to scans and attacks.

References

[1] Akin T.," Hardening Cisco Routers," O'Reilly & Associates, 2002.

[2] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," *In Proceedings International Conference on Advnaced Communication Technology, 2004.*

[3] Chen S., Iyer R., and Whisnant K., " Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors," *In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.*

[4] Kim H., "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, FEBRUARY 2004

[5] Rybaczyk P., "*Cisco Router Troubleshooting Handbook* ", M&T Books, 2000

[6] Jo S., "Security Engine Management of Router based on Security Policy," *proceedings of world academy of science, engineering and technology,* volume 10, ISSN 1307-688, 2005.

[7] Q. Ali., and Alabady S., "Design and Implementation of A Secured Remotely Administrated Network," *In Proceedings International Arab Conference on Information Technology, ACIT'2007.*

[8] Alabady S. , "Design and Implementation of a Network Security Model using Static VLAN and AAA Server," *In Proceedings International Conference on Information & Communication Technologies: from Theory to Applications, ICTTA'2008*

[9] Shastry Y., Klotz S., and Russell R., "Evaluating the effect of iSCSI protocol parameters on performance, " *In Proceedings of the Parallel and Distributed Computing and Networks, 2005*

[10] *" Network Security 1* ", Cisco system,Inc. 2006

[11] Eld G., and Hundley K., "*Cisco Security Architectures*", McGraw-Hill, NewYork, 1999.

[12] Wa Y., "The design and implementation of router security subsystem based on IPSEC," *proceedings of IEEE TENCON'2002*

[13] Riedmuller S., Brecht U., and Sikora A., " IPsec for Embedded Systems, " in: H. Weghorn (Ed.), *Proceedings of the 2nd Annual Meeting on Information Technology & Computer Science at the BA-University of Cooperative Education, ITCS 2005.*

[14] Chapman D., Cooper S., and Zwicky, E.," *Building Internet Firewalls*," 2nd Edition, O'Reilly & Associates, 2000.

Salah Alabady was born in Mosul, Iraq, on October ,1972, he received the B.Sc. degree in Electronic and Communications Engineering from the University of Mosul, Iraq in 1996, and in 2004 he received the M.Sc. degree in Computer Engineering from University of Mosul. From 2004 till now he is being a lecturer in Computer Engineering Department, Mosul University. His research interests include optical fiber communications, optical network architecture, network security and computer networks design. Alabady gets 10 certifications from Cisco Networking Academy, and he is working as Instructor, Curriculum Leader, and Legal Main Contact in Mosul University Regional Academy for Cisco Networking Academy program.

Table 1. Common configuration weaknesses

Weakness	How the weakness is exploited
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and password to snoopers.
System accounts with easily guessed passwords	This common problem is the result of poorly selected and easily guessed user password.
Misconfigured Internet services	A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites, IIS,FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security protocols, or SNMP community strings can open up large security holes.

Table 2. Common security policy weaknesses

Weakness	How the weakness is exploited
Lack of written security policy	An unwritten policy cannot be consistently or enforced.
Politics	Political battles and turf wars can make it difficult to implement a consistent security
Lack of continuity	Frequent replacement of personnel can lead to an erratic approach to security
Logic access controls not applied	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved application create security holes.
Disaster recovery plan is nonexistent	The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise.

Table 3. Identify the threats

Threat	Internal \ External	Threat consequences
e-mail with virus	External origination, internal use	Could infect system reading email and subsequently spread throughout entire organization.
Network virus	External	Could enter through unprotected ports, compromise whole network.
Web based virus	Internal browsing to external site	Could cause compromise on system doing browsing and subsequently affect other internal systems.
Web server attack	External to web servers	If web server is compromised hacker could gain access to other systems internal to network
Denial of service attack	External	External services such as web, email and ftp could become unusable. If router is attacked, whole network could go down
Network User Attack (internal employee)	Internal to anywhere	Traditional border firewalls do nothing for this attack. Internal segmentation firewalls can help contain damage.

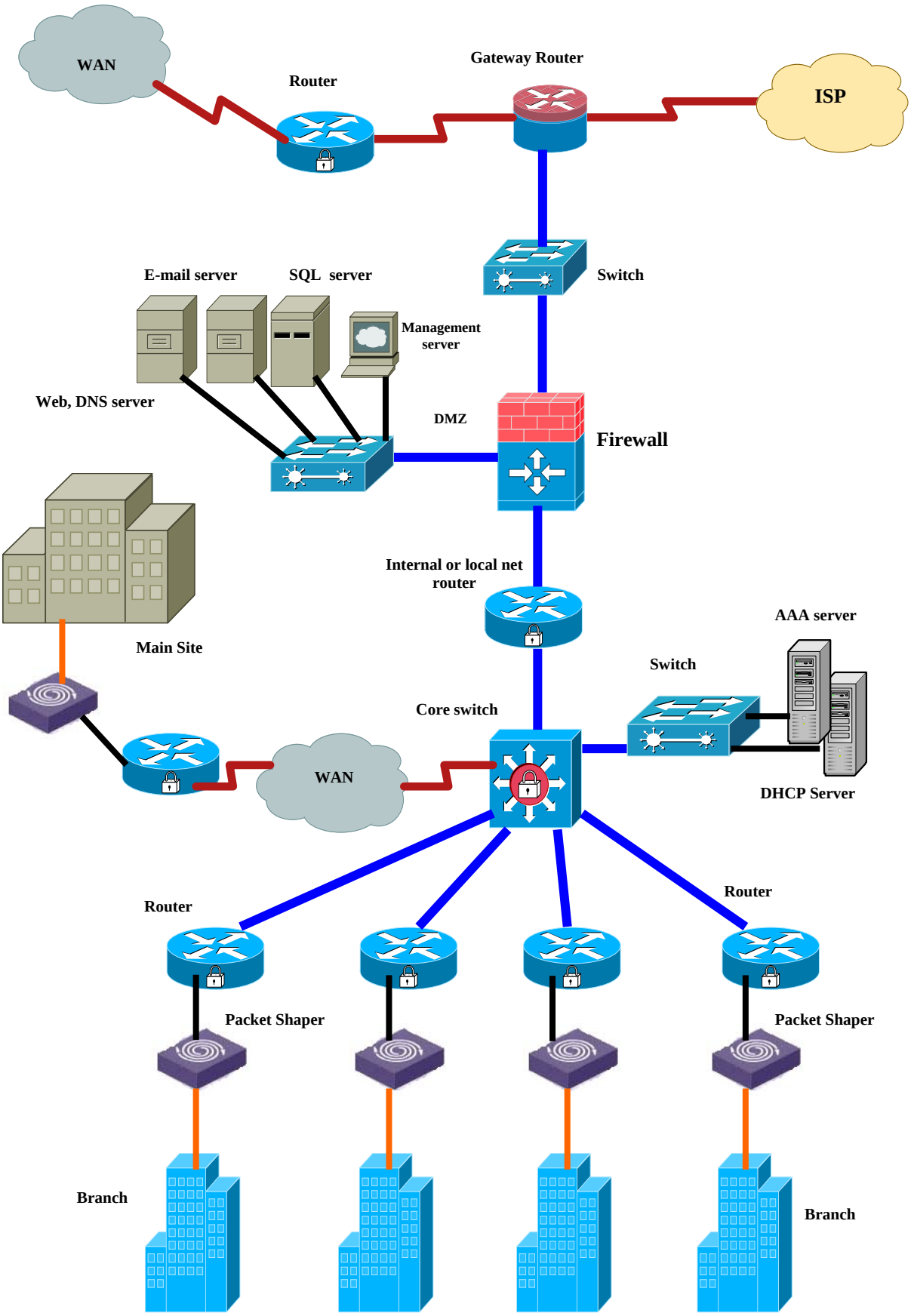

Figure 1. Structure of the suggested network security model

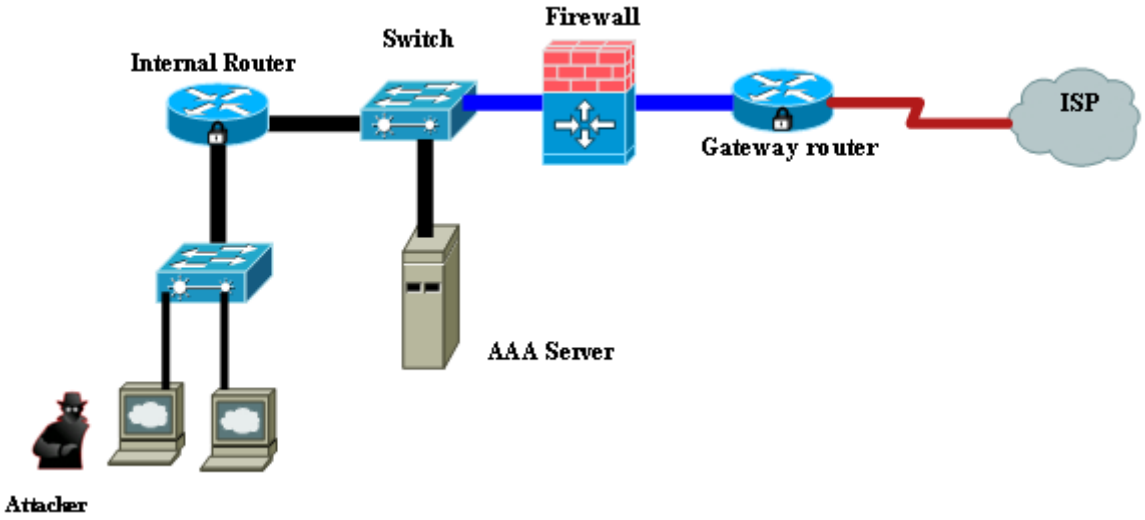

Figure 2. Router with firewall configuration for a network test bed