Global Information Assurance Certification Paper

Sangameswaran.M.V.
GSEC Practical Assignment Version 1.2f
Combating Cyber Terrorism at the Perimeter Level Using Firewalls

The idea of this paper is to give an introduction about firewalls, why it is required to secure the perimeter-level defense of any network, the different threats and types of attacks on the networks, the types of firewalls and different techniques to prevent hackers and unwanted payloads to and from any network and a brief introduction about Symantec Raptor firewall and how it is different from other firewalls.

Introduction

As we are witnessing more and more hacking incidents, one thing is clearly emerging, i.e., Information Security is no longer an IT related issue but it has metamorphosised into a business related issue. In the present day world we can't imagine two countries without a controlled border, as there might not be any privacy or security. Just like that we cannot even think of two networks without any controlled access between them as it fails to ensure the privacy and security of the stored information that is now considered as invaluable assets of any enterprise or network.

The concept of firewalls has evolved over a period of time. According to Indian mythology, "Agni" - which means Fire is considered as the "God of protection". Ancient kingdoms in India used large barriers of fire to act as a protection against the attackers attacking them. Exactly similar is the concept of firewalls. It creates a barrier protection between the inside and outside of any network. As the world of network grows, the enterprises also expand. Together with this expansion, security risks are also on the rise. Any network expansion in conjunction with the growth of any enterprise will obviously result in a number of access points to sensitive information that is of course the prime asset of the enterprise. Each of these points that can be accessed from external network, is a clear representation of a possible vulnerability that may be probably used to gain unauthorized entry into the company's intellectual, commercial and valuable assets. Identifying these key access points is crucial and critical to safeguard an enterprise from hackers, competitors and cyber terrorists.

Even though companies are having private networks, the growth and popularity of internet has urged them to plug in their networks directly to the internet. The main reason being survival as more and more enterprises depend on the internet as a medium to reach their customers and communicate to them effectively. As the net is growing exponentially, more people are getting inside the net, some serious users and some casual users. The more people are getting inside the user-pool, the more secure the transactions should be which they do through the medium of internet. So it has become an absolute must to protect vital information from incidents, regardless whether it is intentional or unintentional or by some cyber terrorism acts. In this paper I'm going to discuss how to prevent attacks into any enterprise network successfully using a firewall as a perimeter level defense tool. One question that remains is that whether perimeter level defense **alone** will protect an enterprise from attackers. The answer is **NO**. Because the basic functionality of any firewall is to act as a security checking point between boundaries of private networks and public networks. About 70-80 % of the hacking happens from within the private network itself. So by all means perimeter level defense alone is surely not going to completely protect any network, as a firewall doesn't know what is happening within the network. Imagine there are different workgroups for Finance, Marketing et.al. within the private network of an enterprise. A

firewall at the single entry point to this large corporate network cannot monitor who from finance is accessing information from marketing workgroup. So tools for vulnerability assessment and intrusion detection are required to act as internal level protections that continuously monitor the internal network. Cryptography and Encryption tools are also helpful in securing enterprise networks.

Categories of Threats

Security threats can be broadly classified as human and non-human threats. Human threats can be further sub-divided into malicious and non-malicious threats. Malicious threats include outsiders like crackers and hackers or insiders like disgruntled employees. Non-malicious threats mostly constitute of ignorant employees who accidentally open certain ports and create vulnerabilities in the network. Non-human security threats consists mainly problems / flaws created by the hardware, software, bugs in the product as well as the OS. These are events that may be open security breaches.

Hackers

These are the people who created the need for firewalls to defend the perimeter of any network. The term "hacker" was at first used to describe someone who knows in and out of computer, but as technology and networks grew with internet and became popular, the word "hacker" started to have a new meaning of a person who is committing a computer crime. Usually a hacker comes into the network by any of the three ways that are known as Vectors of Attack. 1) Attacker can use a computer directly in the private network. 2) He/She connects to the network over the Internet and exploits some vulnerabilities on the firewall or on the network if firewall is not present. 3) He/She tries to dial-in via a RAS server.

Stages in Hacking Attacks

There are 3 stages in any hacking attack, which consists of the following:

System Selection – The hacker first identifies a specific computer system to target. For this stage to pass, it should have made some vector of attack possible by establishing its presence in the open space that is already found using any searching techniques.

System Identification – The hacker then determines the features of the system to be targeted before actually engaging it. This is usually achieved through the information available on the public network. Probing the target to extract valuable information from it using non-attack methods also forms part of this stage.

Attack Mode – Based on the information collected during the system identification stage, the attacker selects one or more specific attacks to be used against the target system and then proceeds with the attack method.

Types of Attacks

Based on the level of skill, knowledge of target and resources utilized et.al., the hackers can be classified into various categories. Some of them are as follows:

Corporate / Government Spies – This category has medium to high level of skills with an equivalent good knowledge of their target. These people have very high resources at their disposal and have national interests, financial as well as competitive gain as the main motivation behind attacking.

Insiders – Even though this category has medium level of skills, they have a high knowledge of their target with a moderate amount of resources for their use.
Cyber Terrorists – These types of attackers have high level of skills with a moderate level of knowledge of the target. These type of attacks are triggered by religious / political ideals as means of motivation.
Hackers can be further divided in to 4 categories as

1) Novice, who are also known as *Script Kiddie*, *Wannabe*. These people have absolutely lots of time and are dangerous because they don't always know what they are doing. All the hacking stages for these people are in low-level only.
2) Black Hat – This category is a malicious one who has a high level of target knowledge.
3) White Hat – Also known as Noble / Old School with medium level of skills & resources with no target. The main motivation for this category is improved security but in the process they write tools, which are mostly used by the novice.
4) Grey Hat – This category plays both the role of black as well as white hats.

There are various information-gathering techniques which attackers use during the stage of target selection and identification. Below mentioned techniques are some of them:

A) IP address scanning – This method does a scanning of the public network and finds out the IPs that are available in the outer space which can be attacked using various other techniques. Utilities like Ping, TJPing, and traceroute are used for this purpose.

B) Social Engineering Techniques – There are different methods in the social engineering techniques itself like

1) Zero-sum knowledge attack - which is baiting someone to add, clarify or deny pseudoknowledge of the attacker, claiming to know more than you do, to solicit more information.
2) Knee-Jerk Response attack – which is presenting an exaggerated lie in order to get an informational response.
3) Stake-out attack – which is the method of analyzing the activity and movement of people over time.
4) The 10 attack – which is the method of using a sexually attractive person to gain sensitive information or access to the critical information.
5) Help-desk attack – This is a simple method but most people fall prey to this method. This method uses the technique of an end-user seeking help to get connected to a particular server or to a specific service.
6) Fake-survey attack – which uses fake questionnaire which asks lot of questions about your network by promising some fake prizes which really woo the people who in turn reveal the info about their network and fall prey for outside attacks.

C) Port Scanning – During the initial phases of identifying a target system, the hacker's intention will be to find out what OS it is running and what are the services being provided to the clients in side the network. As per TCP/IP concepts, any network based on TCP/IP, services are provided on specific sockets. Sockets are a numbered connection that is a unique identifier of the OS and the supported services. There are enough tools available on the Internet that can be used to identify what all sockets are responding to network connection requests. The hacker can then put his effort on ports that has open services running left unsecured. For e.g.: Scanning TCP ports between 0 & 150 and if the result shows a port 139 in the scanned list, then it could be a windows host. Similarly port 135 corresponds to the

presence of NT hosts. Ultrascan and NMAP are tools for port scanning whereas Slow -scan attack is used to avoid detection of port scanning.

D) NSLookup and DNS Range Grabbing – Services like Finger & Whois are popular among hackers as they provide the account name and personal information for users of the network computers. Even though these services are useful in providing the contact of the people of the enterprise that should have been used by the external users to contact them, hackers use this to break into accounts, usernames and passwords. The hackers also use *traceroute*, written by Van Jacobson to trace the route of IP packets from the source system to the destination and clearly shows the hops that it makes.

The use of these services can always be limited but the same cannot be said about the DNS service. By default, Win NT does not support Finger or Whois. It needs separate software package installation that the network administrator should really think twice. A DNS service is a must in any network, as the internet client software requires it to convert user -friendly domain names like www.oracle.com into machine-friendly IP address like 202.177.163.206. Many large networks thus require a DNS server behind the firewall for internet name service translation.

Hackers use a DNS service to realize the topology of any network. As DNS has a record of all the IP addresses & internet names of all the servers in the network, anyone trying from outside / inside can obtain the details of the most critical computers in the network. The NSLookup is a tool for interrogating DNS servers and by fine -tuning the tool a hacker can pretend as if he/she is a peer DNS server to extract further in formation. The best practice in security against this type of attacks is to allow computers from within private network to access the DNS servers to get the information they need and prevent systems outside your perimeter from getting that information.

As DNS is a hierarchical service, if one DNS sever does not have the answer to a query, it will direct it to the next server up or down the DNS tree. So in a large network, a DNS server within your perimeter might be required to contact a DNS server outside the firewall. Compounding to this, many web sites will not respond to Internet requests from clients that don't have reverse DNS mappings. So the web -servers need to contact your DNS server through your DNS tree or through their DNS server. All these issue s can be solved using a firewall with NAT (Network Address Translation). NAT will hide the IP address of internal systems by translating it. This is also known as IP masquerading. NATing will make all the requests going out from your network appear as if a ll of them are coming from a single IP. You can also configure a rule in the firewall that allows only the requests from a DNS server up/down your hierarchy tree. Disabling Zone Transfers within the private network is a good security practice.

E) SNMP Data Collection – This is another way of using SNMP that is intended to manage big TCP/IP networks. Hackers use this to get data about your network and then may reconfigure your network to deny a specific service or may even re -route sensitive data out of your network depending on the SNMP features which the hacker has control.

F) Denial of Service – This is an easy attack on any network first by disabling some services. Most of these attacks affect networks based on TCP/IP. The reason being TCP/IP is a widel y used networking protocol and the hacking happens through the internet and the net is also based on TCP/IP. The various methods employed in this type of attack are:

1) Ping of Death – In this method, a specially constructed ICMP packet that violates the construction rules can crash the target server. This happens only if there is no checking for invalid ICMP packets on the target. The best way to escape from this attack is to create a rule in firewall, which denies ping through it, and secure the OS that is not susceptible to ping of death.

2) SYN Attacks – SYN attacks (Synchronize Connection Established) is the way in which hackers overload the network with illegitimate information requests or connection attempts. The initial IP packet of any TCP connection attempt is easy to generate (with the SYN bit set) and simple. Responding to a SYN attempt takes more time to compute and memory allocation as the receiving server should store the information and allocate memory for connection data. Usually the attacker sends one SYN after another to the target computer, which will be made respond to that illegal SYN attempts than compared to legitimate users. All the available time of the target computer is spent on just processing the SYN requests. ICMP (Internet Control Message Protocol) flooding is also another network protocol attack. Here the attacker sends a stream of ICMP echo requests to the target computer, which spends most of its time just responding to these echo requests. You can configure your firewall to monitor or log events of extremely frequent SYN connection attempts or abnormally high traffic of ICMP and protect your internal network.

3) Service Specific Attacks – A hacker is more interested in shutting down one of your services that you are running and then impersonate it. Even though you are having many services that may be attacked, the hackers are mostly attracted to either basic components of TCP/IP or windows networking like RPC, NetBIOS, DNS and WINS. Each of these specific services allow the network clients to connect to them on specific ports and for each service, the data expected is in a specific format. So hackers send incorrect messages to the network services to crash it and it is difficult to trace back them especially if they are using the technique of source routing. Some DNS servers crash if they receive a DNS response without even sending a DNS request first.

G) Impersonation – This is another method used by hackers to get into any network. The hacker first snoops/eavesdrop into your network traffic to get enough information to log onto your network. If this is not working, he/she may use a DoS attack that creates a loophole as the other computers in your network might reveal the required information for the hacker to get inside your network. There are various tactics for this as:

1) Source routed attacks – In this tactic, the attacker sends data from one source and makes it look like it comes from another trusted computer. Even though source routing is a useful tool for network diagnostics, hackers exploit this option. This can be disabled in the firewall to drop all source routed TCP/IP packets from the internet

2) DHCP service impersonation – If the client computers are configured to get configuration information at boot-time, the hacker can penetrate into the network and impersonate that service which may create havoc. Suppose there is a DHCP server, the hacker can impersonate it and redirect all the clients to talk to any hostile hosts under the hacker's control. The same is applicable to both DNS & WINS services too. This attack happens only if the hacker has gained control of any computer and then launches a DoS attack against DHCP, WINS or DNS and then impersonates it. So this type of attacks relies on other attack methods to be successful. The defensive measure should be to prevent DoS attacks at the perimeter level itself.

H) Man-in-the-Middle – This type of attack is a special case of impersonation attack, in which the hacker just slides in between any two computers within t he network or between an inside computer and an outside server in the internet. When a client opens a connection session with the server, the hacker intercepts it either through DNS or DHCP impersonation attack or by re-routing the IP traffic from the clie nt to the hacker's computer, which in turn opens a connection on behalf of the client computer with the server. Both the client and the server computer will think that they are communicating with each other, whereas the hacker in the middle will be able to observe and may modify all the communications between them. The protection for these types of attacks is the use of strong encryption.

I) Session Hijacking – In this type of attack, the hacker grabs the already established and authenticated session. This can occur at TCP connection layer and at the SMB or NFS session layer. The hacker should be able to predict TCP sequence numbers in order to grab an existing TCP connection to keep the IP packets in order to ensure that they all arrive at the destination. He/She should also be able to re-route packets as well as launch a DoS attack to make sure that the server does not sense anything wrong.

Firewalls and Perimeter-level Defense

A firewall is a system that mainly operates as a security gateway separating two networks. On one side you have a public network which can't be controlled just like that because we can't predict what is being done out there, when and how. On the other side, you have a private network that has the most critical and important informa tion about that enterprise. Some may even have web-servers that are kept in the DMZ (Demilitarized Zone). DMZ is a segment of the network that sits between the internet and an internal network's perimeter defense. Usually, the DMZ contains devices accessib le to inbound traffic from the internet such as web-servers, FTP servers, SMTP E-mail servers and DNS servers.

Most of the attackers focus on the exploitation of any known vulnerabilities of any service pertaining to specific implementations and then atta cking that. As firewalls are designed to lock some of these vulnerabilities out, it can act as a useful tool for perimeter level defense. Firewalls occupy an important position just at the borders of your network, where it is providing gateway access to ot her public networks and allows you to assign specific services to specific systems that are allowed and optimized for that. As the traffic between internal and external networks should necessarily pass through the firewall, it may slow down the traffic. But considering the safety that the firewall is providing, this performance degradation can be compromised. The rule is " To gain something, you have to sacrifice something! ". Firewalls can either be a hardware, software or a combination of both.
Typically the functions of most firewalls are as follows:

- Providing perimeter level defense to a protected private network.
- Restricting and controlling access in both directions
- Implementing technical traffic-flow control
- Generating logs about packet and connection events

But it should be noted that firewalls do have some limitations, as they don't protect

1) Against viruses coming through HTTP/FTP/SMTP traffic
2) Connections that bypass the firewall
3) Against unknown threats
4) Against internal threats / neither abuse nor provide physical security.

Firewalls give tremendous power and capability to the security administrator by specifying which employee should access what service. He/she can create a security rule such that only one person will be authorized to use an FTP *puts* command and another one to use *gets* command. In progressive firewalls it can even be specified the time ranges and allow browsing to specific sites only during that period. A proper security policy that is clearly drafted and enforced ensures that the perimeter of the protected network, which has lots of sensitive information, is secure. The architecture should be in such a way that the firewall should be the gateway for all traffic between the secure private networks, which is under control and not so trusted external public networks like the net.

Types of Firewalls

Simple Packet Filter

These types of firewalls were the first. In the fourth layer of OSI standard i.e., the transport layer, these firewalls analyses network traffic. Packet filtering fire walls are able to protect unwanted IP packets or block them based on specific characteristics like source/destination IP addresses, TCP/UDP ports or TCP flags. There are rules, which are created specifically based on data-link, IP, UDP and TCP headers. The firewall reads the source, destination and protocol information from the header of each packet. As the packets start to move in and out of the network, it is compared against the defined rule set for one or more protocols like TCP, IP and ICMP. If the pac ket satisfies all the rules, which are maintained in TCP/IP kernel, it moves up the network layer for further processing. Usually the TCP/IP kernel rule set will be having an allow/deny list and a packet needs to go through these lists and get checked whether it has to be allowed or denied. When a packet arrives, it also checks for the rule, which specifies that particular protocol -port combination. There should be a specific mention about ICMP protocol, as it doesn't use port numbers for communicating. In this case it is difficult to apply any allow/deny rules just like that. Using state -tables, which ensure that an ICMP reply was requested from a host in the inside, network, we can apply the allow/deny rule-set on ICMP protocol. Packet filters typically us es command sets, which does all the filtering according to the firewall state -table. As packet filters are implemented in network layer, it doesn't know how to process an application level protocol like an FTP/HTTP request. When the packet reaches the filt er, it is inspected for any matching rule in the rule - base, if there are no matching rules, then the packet is dropped and if there are matching rules, then the communication is allowed. This uses TCP/UDP port filtering.

Packet filters have many advantage s. As it performs only limited checking using the rules defined in the rule-set, the packet filtering firewall is fast. It is usually implemented in hardware components as packet routers (For e.g.: - Cisco PIX. It also supports stateful inspection). As a s ingle rule will drop packets that are not supposed to go out of the internal network, it secures the entire network. There are no major configuration changes required at the client side as the packet filter does the entire configuration by itself. When use d with NAT, it hides the internal IP from outside network.

Even though packet-filtering firewalls are fast and simple to use, it has many disadvantages. The first issue is its inability to understand application level protocols such as FTP and HTTP. Becau se of this it can't monitor FTP *puts* and *gets* commands that may be used for some communication with the public network. Payload of the packets is not checked by the filter and the decisions for either allowing or denying is not based on the packet contents that can be dangerous. Imagine a packet filter with SMTP allowed. An e -mail virus/Trojan can come through the path and attack the network. Packet filters inspect packets in isolation and

does not maintain state information. It doesn't have any application features like URL filtering and user authentication. It has a limited handling of complex policies. The user interface for rule configuration is a difficult one. The logging and alarming functions are inadequate. The main disadvantage of any packet level firewall is that it is susceptible to application level as well as routing -based attacks. The hassle of creating rules in the proper order is a headache as an improper order may result in a serious security breach.

Stateful Packet filtering Firewalls

A stateful packet filter collects and maintains information on each packet that passes through the firewall on connections. This information is then used to track open valid connections without reprocessing the rule -set for each and every packet. In this meth od, only the first packet of a TCP connection needs to be approved. Once a session is established, later TCP packets are recognized as part of the same connection. A stateful filter can implement complex policies and has extensive logging and alarm functio ns. The user interface is easy to use when compared to simple packet filter firewalls. The drawbacks of stateful inspection firewalls are that there is a susceptibility of application layer attacks on the protected network and it lacks proper user authent ication control. The stateful packet filter cannot check the payload of packets and does not retain the state of connections.

Application level Proxy Firewalls

Application level proxy firewalls have a set of in -built proxies into it, which imitates both ends of the network connection. This evaluates the packets for a valid application data at the application layer even before allowing to get connected. All the state and sequencing information is maintained after examining all the packets at the application layer. The proxy services which come with this firewalls let the security administrators to manage the traffic flow using a specific proxy like HTTP, FTP or TELNET through the firewall. This provides a greater level of security using access control, passw ord authentication and detailed inspection for valid data.

The application proxy always does complete analysis of the command set at the application layer. Whenever an incoming packet is received, it checks for the header information in the packet and processes it at the transport layer stack. Thereafter the payload found in the packet moves up the stack to application layer where there is proxy server which listens to specific TCP/UDP port. The next step is the processing of the payload in the packet. Thi s information is then compared to the rule set, user access permission rules and host access rules and if it matches, the proxy accepts the payload packet otherwise it denies the request.

The proxy services of an application proxy firewall works like this : - for each application like HTTP, FTP and TELNET, there will be an application proxy in the firewall that consists of a server part and client part. The main purpose of this architecture is such that the users from the trusted private network should not be allowed to access any outside server directly using any application and all traffic should compulsorily pass through the proxy. When a system inside the private network wants to connect to the public network using an application like FTP, it sends an FTP request to the FTP proxy server. The proxy server in turn inspects the header, checks the rule and passes the payload to the application proxy which compares with the allow/deny rule -set for the particular network connection and the packets should necessarily contain the protocol details. Once the request is allowed the FTP proxy client requests a connection on behalf of the system in the private network which had requested a FTP connection with the original FTP server in the public network. Once a connec tion is established between outside FTP server and FTP proxy client, the client passes on the

response to the FTP proxy server that in turn sends the response to the original client inside the private network that had requested for the FTP connection. The proxy service is transparent to the private network as well as the public network as both sides will sense as if the request and response are coming directly to them.

The strength of an application proxy firewall is that it never allows a direct connection between any systems in the private network to the public network like Internet. It can also allow/deny any initial connection request. The strength of connection verification using user authentication also adds on to the advantages of an application proxy firewall. Application proxies are much slower when compared to packet filters as each packet in any session is put on to thorough check. Each packet should go through the low-level network protocols till the respective proxy finally inspects it at the application level and sends back to the network layer down. So the application layer checks on the packet to ensure that it is never spoofed. Application proxies also do NATing to prevent exposing the private IP addresses to the public network.

As the proxy services operate in the application layer and on top of the operating system, these are vulnerable to the OS as well as application bugs and application level proxies require seamless support from the OS to run correctly. These include TCP/IP, Win32, Winsock et. al. For any protocol to pass through the firewall, a proxy needs to be added to the firewall. As the application and its proxy process inbound/outbound data, the speed will be slow; but considering the level of security application proxy provides, it can be compromised.

Let us take a case study of an application level firewall like Raptor firewall from Symantec Corporation and analyze how it is different from other firewalls. Raptor firewall (previously known as Eagle firewall) has the following unique features. Raptor is an ICSA certified firewall. (Please visit http://www.icsa.net for details on other firewalls also).

OS hardening

Hardening an OS means shutting down unnecessary services and patching all security holes. Raptor does OS hardening while installing itself. It performs a series of checks and performs the following actions:

- It disables IP forwarding/routing on the firewall and all non-IP protocols like IPX.
- It disables all non-administrator accounts like Guest and User.
- All IP based services not required on the firewall are disabled (for e.g.: NFS, ECHO and CHARGEN).
- It adds IP level code to the IP stack (Shim) to prevent various IP level attacks like source routing, IP spoofing, SYN flood et.al.
- It disables all unnecessary services/processes.

Apart from installation OS hardening, Raptor does continuous system hardening. Raptor comes with a daemon known as "Vulture daemon" which continuously monitor, detect and disable any new unauthorized services/processes. It disables IP forwarding/routing at all times, disables any non-administrator/non-root logins. It also detects port scans, which is a familiar method among hacker community. This automatic hardening is a feature of Raptor.

Non-order dependent rule set

This allows the security administrator to create rules in any order without creating any loopholes for security breaches. This feature of having non-order dependent rules makes

Raptor firewall unique. Other firewalls have order dependent rule sets that should be configured at various places/levels. This is often confusing and in -turn creates security lapses.

Single GUI
Firewall can be managed either locally or remotely using a single GUI known as RMC (Raptor Management Console). It has different us er-friendly wizards to create rules.

Blocking FIN scanning attacks
The default rule set in raptor does not allow FIN scanning where as other firewalls have the default rules which allows FIN scanning to occur (it does have a symmetric multi -processor support). Raptor can also be used to block buffer overrun attacks in HTTP and SMTP. Raptor prevents ICMP being used as a covert channel. In other firewalls, ICMP is enabled by default rule set.

No potentially exploitable services in the firewall
Raptor does not allow by default any potentially exploitable services like SMTP on the firewall. E-mail is already an easy way of attacking any network by email bombing. Email bombing means sending many copies of the same email to a specific address and email spamming is sending the same email to many addresses. All sorts of spamming can be controlled on the firewall proxy services itself.

HTTP content blocking
Raptor is integrated with webNot to perform content filtering to restrict employees from browsing unwanted co ntents. These blocking rules also can be based on users, groups or IP addresses for further enhancements. (For further info on HTTP protocols go to http://www.w3.org/protocols)

Blocks unauthorized connections
Raptor blocks all unauthorized connections like FTP connection even after the FTP session has terminated. Other firewalls don't check for this vulnerability.

Strong user authentication:
Raptor has strong user authentication methods by means of Defender, Se cureID, RADIUS, TACACS+, S/Key, gwpassword, NT domain etc. It also has a feature called "out of band authentication"(OOBA) which is useful as an authentication mechanism for protocols that doesn't support standard authentication. For e.g.: SQL*NET.

Wide range of application proxies
Apart from the common proxies like HTTP, FTP, SMTP, Telnet and Rlogin which most of the other firewalls have, raptor has separate application proxies for ping, SMB/CIFS, login/shell/cmd, SQL*NET, Real Audio, H.323, NTP and NNTP. This adds up to the hybrid architecture that does application proxy, packet filtering, stateful inspection and circuit level proxy.

Logging and alerting
Raptor has detailed logging for each and every attempt regardless whether it was allowed/denied. Eve n logging can be disabled, but it is not advisable to do so as tracking the traces of an attack would not be possible. For alerting, raptor has various methods like email, sound alert, pager, phone and SNMP traps.

Note- For the latest list of vulnerabili ties in any firewall please visit http://www.secuityfocus.com or http://www.securitytracker.com

Above all, the most important point is that the firewall should su pport the security policies of the enterprise rather than enforcing it. People should realize that security is an investment and not an expense and some level of security is better than nothing.

Conclusion

Although different types of firewalls maybe able to safeguard the perimeter level of security of an enterprise against cyber attacks, there are also other security threats like insider abuse and internal hacking within the enterprise which the firewalls can't detect. So, for securing the enterprise networks from inside threats too, tools like intrusion detection and vulnerability assessment are required which make the network safe to a large extent.

References

Internet References:

How Firewalls Work - Tyson, Jeff 2001
URL: http://www.howstuffworks.com/firewall.htm

A Comparison of Packet Filtering vs. Application Level Firewall Technology - Ernest Romanofski –
URL: http://www.sans.org/infosecFAQ/firewall/app_level.htm

Securing the Perimeter, Part 1 – Author Unknown
URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=743&PID=8200610

Securing the Perimeter, Part 2 – Author Unknown
URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=783

Firewalls Complete - Marcus Goncalves
URL: http://secinf.net/info/fw/complete/

Application Layer Firewalls vs. Network Layer Firewalls: Which Is the Better Choice? - Keith D. Maxon
URL: http://secinf.net/info/fw/firewall.htm

Unknown. "Application Proxy vs. Stateful Inspection Firewall Technology." June 1, 2000
URL: http://www.firetower.com/forum/applicationproxy.html

Securing the Internal Network from the Internet Perimeter with a PIX Firewall: Another Layer of Protection - Naeem Qasim
URL: http://www.sans.org/infosecFAQ/firewall/PIX.htm

Check Point Firewall-1's Stateful Inspection - Michael J. Nikitas
URL: http://www.sans.org/infosecFAQ/firewall/inspection.htm

Firewall FAQs
URL: http://www.faqs.org/faqs/firewalls-faq/

Raptor Firewall 6.5 Running on NT 4.0 - Dennis Carter
URL: http://www.sans.org/infosecFAQ/firewall/raptor.htm

e-Security Guide from Symantec Corp. – Author Unknown
URL:
http://enterprisesecurity.symantec.com/SecurityServices/factsheets/esecurityhandbook.pdf?PID=8200610

http://www.checkpoint.com

http://www.securityfocus.com

http://www.securitytracker.com

ICSA certified list of firewalls
URL: http://www.icsalabs.com/html/communities/firewalls/certification/vendors/index.shtml

http://www.w3.org/protocols

Book References:

Firewalls 24Seven – Matthew Strebe & Charles Perkins ISBN: 0-7821-2529-8 Publishing Date: - 10/99

Symantec Raptor Firewall Implementation Guide Version 6.5 for NT

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor