Global Information Assurance Certification Paper

"Basic firewall configuration and taking advantage of basics IDS characteristics in Netscreen firewalls"

Author: Marco Antonio Balboa S.
Date: September 17th, 2003

Abstract

In this paper I attempt to explain briefly how to take advantage of the basic IDS characteristics in a Netscreen firewall, to make a network administrator without an advanced knowledge of how to block different attack types, and with a simple firewall configuration secure the network in a serious manner. In this case, we will take as an example the basic IDS characteristics that has the Netscreen firewalls. I don't attempt to do any kind of advertising for the product or the Company; the purpose of this paper is merely educational. Through this paper I will try to explain how to configure the firewall through the web interface and show how to enable in a simple and proper way the basic characteristics of IDS in a practical example for a little company with a SOHO network.

Table of Contents

Introduction 2
What are firewalls? 2
Packet filters 2
Proxy Application 2
Stateful Inspection 3
What are IDS? 3
Firewall Netscreen 5XP Elite 4
Characteristics of the Company 4
How the company works and how the problem began 4
Proposal 5
IP Change to private type 6
Firewall Installation 7
Services Publication 7
Main management console 8
Basic firewall configuration, outgoing and incoming rules, practical example. 9
Basic configuration of the IDS characteristics, personalized configuration for SOHO network 12
Flood defense
ICPM Flood 13
UDP Flood 13
SYN Flood 14
Alarm Threshold 14
Source Threshold 14
Destination Threshold 15
Time out 15
Queue Size 15
Blocking HTTP, Java, ActiveX components 15
MS-Windows Defense 16
Scan / Spoof / Sweep Defense 16
Denial of Service Defense 17
Ping of death Attack Protection 17
Tear-Drop Attack Protection 17
ICMP Fragment Protection 17
Large Size ICMP packet (Size > 1024) Protection 17
Block Fragment Traffic 17
SYN-ACK-ACK Proxy Protection 18
Source IP Based Session Limit 18
Destination IP Based Session Limit 18
Protocol Anomaly Reports -- IP Option Anomalies 18
Protocol Anomaly Reports -- TCP/IP Anomalies 18
Conclusion 18

Introduction

In this paper, I will cover how a network administrator with a limited knowledge of security, can configure a firewall and customize their basic IDS characteristics. At the beginning, I will explain briefly first what are the firewalls and their types. Also I will explain what is an IDS, show how the firewall Netscreen 5xp elite has those basics IDS characteristics and how customize them for a fictional company. In the process, I will explain shortly the firewall configuration for that company, we will concentrate in the IDS customization and explain how the attacks work and that the firewall can protect the network against it.
It will be very important for this paper to explain first what is a firewall and what types exist, also briefly explain what is an IDS, because the firewall which we want to configure and customize is one the that has those characteristics. We want to help a network administrator how to configure easily and shortly. For an advanced and detailed configuration, I show footnotes that can help in a detailed configuration.

What are firewalls?

Firewalls have been widely discussed, these network devices demonstrated through their development a great importance, and it restricts or allows access from and to our private networks. A firewall is the first network device that should exist as an entrance to the security perimeter into our private network.

Through firewall's history, different types were developed and improved, among which we will mention[1]:

Packet Filter:

This type of firewalls are recognized primarily for filtering the access by rules configured by the user, the same ones that we can find and configure in basic router rules. The problem of this type of firewalls is that they are susceptible to IP Spoofing; this means that the authenticity of the source IP address could not be controlled or guaranteed (IP spoof).

Proxy Application:

As its name says this type of firewall resides at the seventh layer of OSI model. This means that this is an application that works to connect to networks (usually private network and the Internet) forcing all the traffic to pass through the computer with a proxy application. This makes the traffic be inspected and authorized through the proxy application, and this way we isolate and protect one of the two networks connected, preventing unauthorized access from another network.

[1] Netscreen Technologies, "Implementing Netscreen Security Gateways 4.0", (April 2003) Security Concepts, slide 9.

Stateful Inspection:

This type of firewalls have better control over connections, this controls the state of the connections verifying all the packet fields. It means that it checks the address of source IP, destination IP, ports, protocols, sequence numbers, etc.
It exists other types of Firewalls, which are a mixture of these types of firewall or others. Its application can be made by software or hardware, but we will limit to those three in our explanation of the diverse types of firewall.

We have now an idea about what is a firewall, but what kind of firewall does our network need? The firewall needs to have a mixture of the best characteristics of all those kind of firewalls that exist at the time. It would be better if the firewall was hardware designed specifically to be a firewall (appliance) with their own and proprietary software. All these additional characteristics will give our firewall a better performance but what if our firewall has additional IDS characteristics.

What are IDS?

An IDS is an Intrusion Detection System. An Intrusion Detection System sends alarms due to unexpected behaviors of network traffic and standard protocol behavior. The change of behavior of determined protocol activates an alarm and an action is taken by the IDS. As an example, the arrival of a packet with FYN flag activated with a source IP that does not have an initiated connection could cause an alarm, as consequence of an unexpected behavior of the TCP protocol, as well as in the capacity of recognize determined type of attacks, analyzing the traffic and comparing it with different attack types that are stored in a database[2].

Now we have an idea about what are an IDS, I will explain now how the Netscreen firewall 5xp Elite can help us in an easily and shortly manner, because it is a firewall and also has a basic IDS characteristics.

[2] Netscreen Technologies, "Netscreen Intrusion Detection and Prevention v2.0a2", (093-0724-000 2003), pages 2-7,2-8

Firewall Netscreen 5XP Elite

Netscreen Company develops its activity primarily in security devices for networks, especially in the development of firewalls and IDP (Intrusion Detection and Prevention). We will concentrate in the configuration of the smaller firewall model of this company, the 5XP Elite[3]. This model is thought for SOHO networks, Netscreen develops the technology for their firewalls based in ASIC processor. The characteristics of web configuration make the implementation of these firewalls simple, that simple configuration and the basic IDS characteristics make our SOHO network a little more secure. Its simple administration will help us arrive to the requirements of implementation, configuration and personalization within a short time for a SOHO network.
For educational purposes, we will explain the firewall configurations and its basic IDS characteristics, personalizing the configuration for a small and fictional company called "Developers".

Characteristics of the Company

20 Educational software developers
1 Link to Internet of 1Mb
3 Linux servers
- 1st with web server and mail server
- 2nd Domain controller, DNS
- 3rd File server and backup

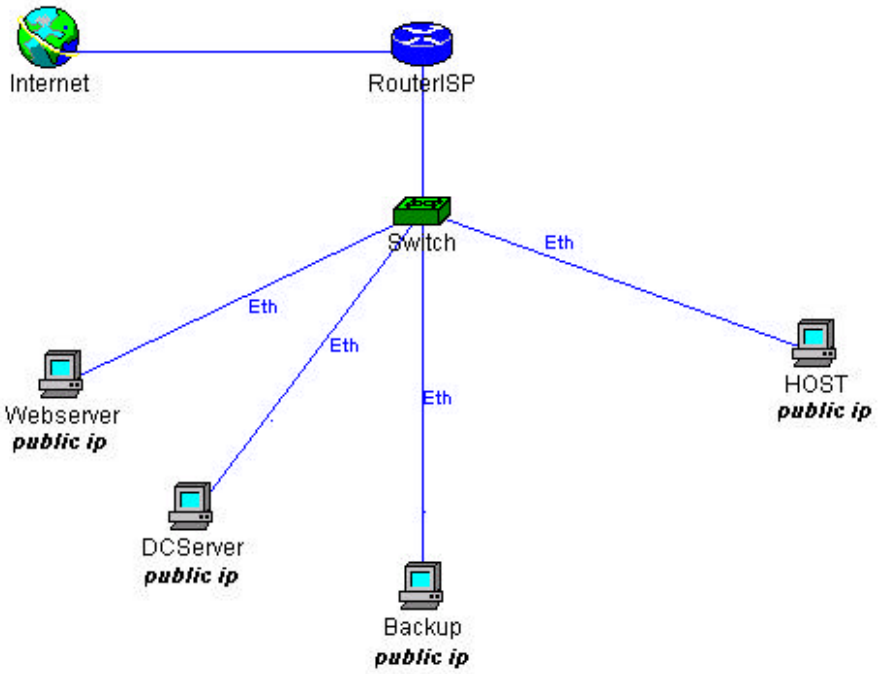
20 computers with Linux

How the company works and how the problem began

The "Developer" company has as primary function to develop computer programs for educational purpose. They advertise their developed applications through Internet using their own web server; their communication to Internet is through a 1Mb link. The company has public IPs for their 3 servers and the 20 workers that develop the educational software. This company never took in consideration the security of its data until they started to realize strange activities in their servers and desktop computers.

The first thing that we have to do is plan a proposal to start securing the company network, so I choose to cover the proposal en 3 steps.

[3] Netscreen Technologies, "Product Capacities Netscreen 5GT, Netscreen 5XT, Netscreen 5XP" URL:http://www.netscreen.com/products/at_a_glance/5xt_5xp.jsp



Graphic # 1

As we realize, this is not the ideal situation for any company that takes its security seriously, for which we will have to make some changes in a way to allow this company to be secured in a minimum but serious way.

Proposal
1st
Change of IPs to private type

It is important to hide the private network of the company, servers and desktop computers to avoid their complete access from the Internet. At first instance, our data such as our fileserver will only be accessed by the company personal integrated at the same LAN. We also have to publish our web and mail server just with 80, 110, 443 and 25 ports open, and in our servers we have to check if there are some other ports opened by a default installation. A general check-up should be realized to secure these servers. We could recommend the use of Bastille, which is a tool made to help secure Linux computers that were installed and left with a default configuration. Bastille will help the network manager with little knowledge of security and Linux reinforce his computers without the necessity of knowing extensively how to perform this task, because it is not the purpose of this paper to give details to the reader of how to secure Linux. We suggest to secure the Linux box in a simple, basic and serious way with Bastille-Linux[4].

[4] Bastille-Linux, Jon Lasser - Lead Coordinator, The Bastille Hardening System attempts to "harden" or "tighten" Unix operating systems URL:http://www.bastille-linux.org/ .

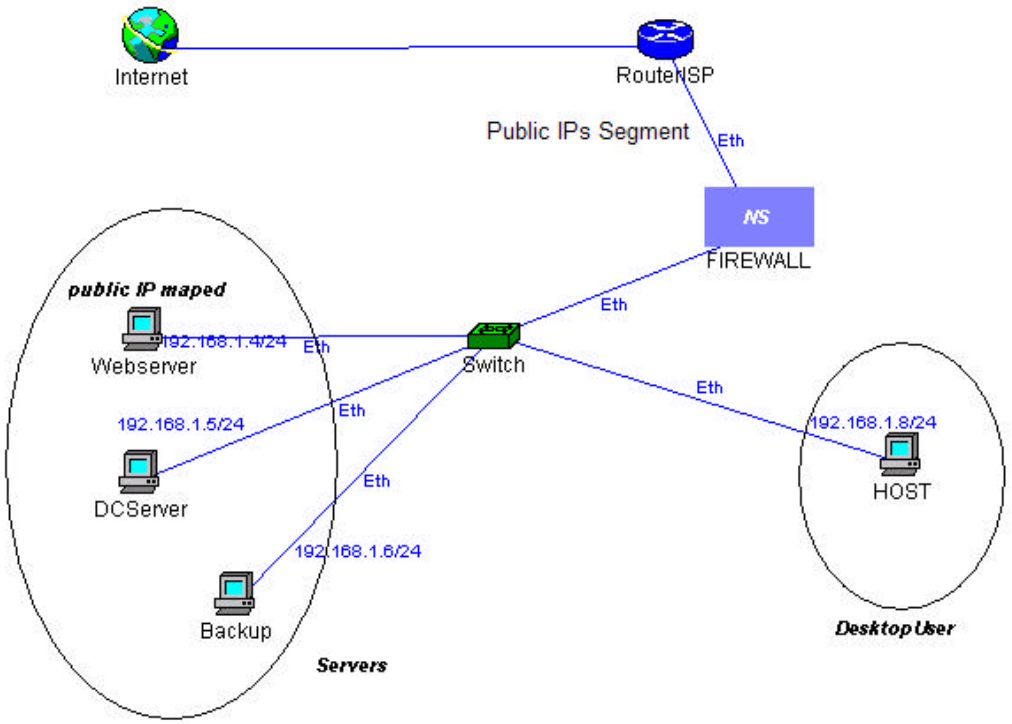
2nd
Firewall Installation

For the firewall installation, we will take in consideration the following; first it will be placed physically between the ISP router and the internal switch of the company. This will have the NAT services configured to avoid external users to access directly the internal computers and secure the firewall with an implicit policy, which establishes that all that is not expressively authorized, is prohibited. So if we do not define a policy of access from the exterior to the interior, no packet will be allowed to enter our internal network. However, we have to establish a policy to publish our web services and mail services.

It is also necessary for the traffic that travels from the interior to the exterior of the company to be allowed only the strictly and necessary services. By doing this, we will avoid the use of programs that can expose our internal network. This rule will deny the use of messaging programs, transference of files with peer-to-peer programs, use of IRC programs, etc. This will only allow the use of http, mail, DNS and FTP. It is important to notice that allowing the strictly necessary services we will avoid the productivity decrease

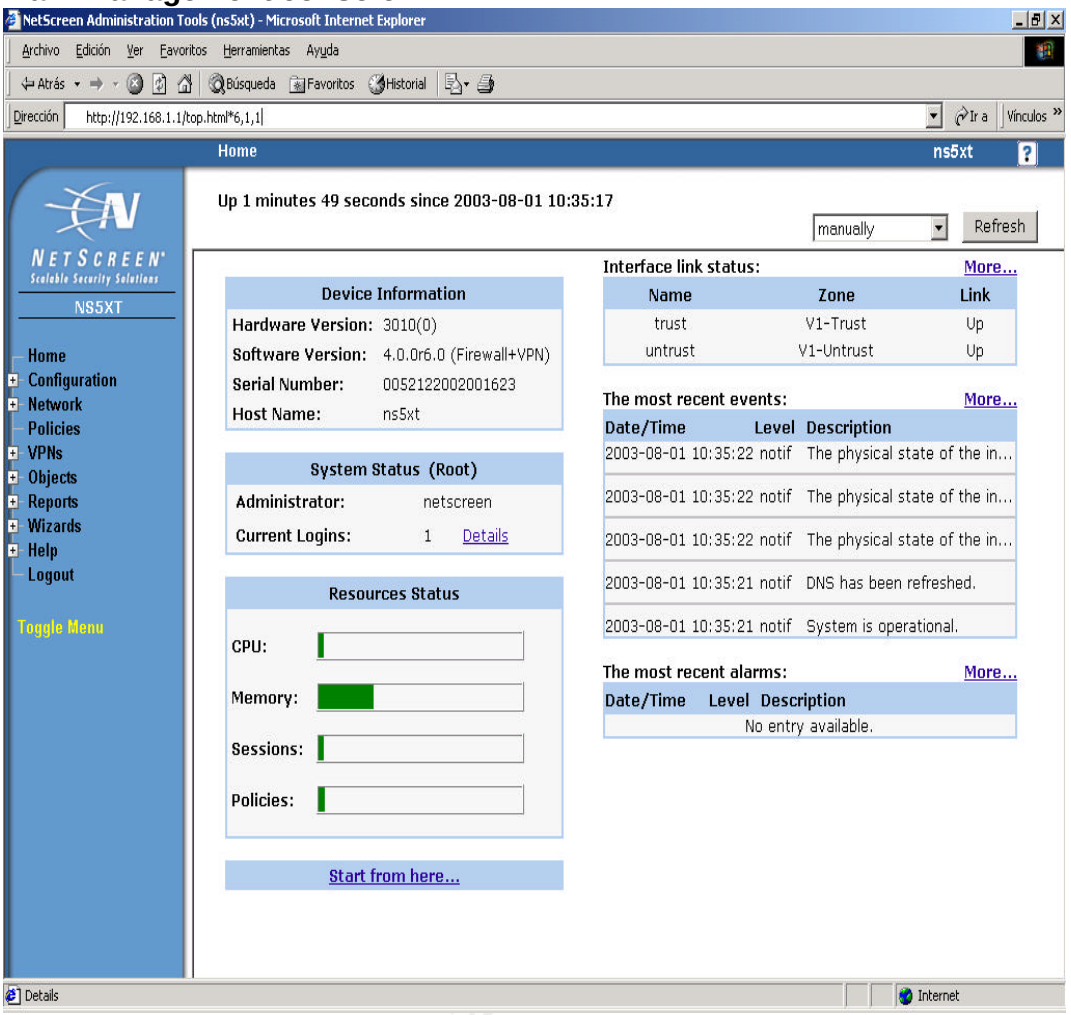
3rd
Services Publication

The only configured services published will be the web server, which means that the only services published are the web and mail. Having our server with a private IP, we will need to configure the mapping of public IP to the private IP in the untrust interface of the firewall so that it can redirect all the http and mail request to the private IP of our server.



Graphic # 2
(Idea of how to secure the network)

Main management console



Graphic #3
(Main management console)

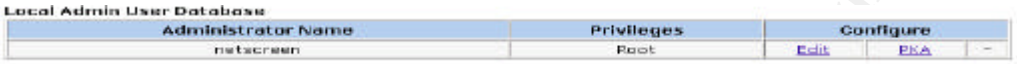
The third graphic shows the main management console via web. In the right frame, we can find basic information such as recent events, recent alarms, the state of the CPU, memory, rules, and session resources, and how many administrators are logged on for the management of the firewall.

Basic firewall configuration, outgoing and incoming rules, practical example

Now we will show how to configure the firewall[5]. The initial access to the main management console of firewall comes restricted by a user and password set by default. Our first task is to change the default user and password to a complex one, this configuration is realized in the following section of the menu.

Configuration→ Admin→ Administrators

Editing the actual user



Graphic #4
Editing default user and password

And changing the name and password by default, for more detailed explanation about how to handle passwords please refer to SANS, GSEC content, Password Assessment and Management, Section 1.2.3

Graphic #5
Changing the default user and password

Once we change this, we will define the objects, which we will have in our network to which we will be allowed or denied an access. We will attempt not to enter into details of this matter because the principal purpose of this research is to expose the characteristics of IDS and not the configuration itself.
For now, we will configure all our list of internal objects (attached to the Trust interface)

Objects→ Addresses→ List→ Trust

The addresses must be created within the zone that will reside after they are grouped by function to facilitate the creation of policies. In our example we create the addresses of our desktop computers and servers and associate them in groups. For example, if we desire the HOST groups, then we will pass to create an outgoing policies.

[5] Netscreen Technologies, "INSG Course, Implementing Netscreen Security Gateways v4.0,", (April 2003) Chapter 13, page 213.

Policies–> From Trust to Untrust

From Trust To UnTrust

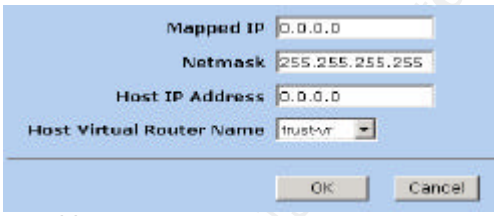
ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
0	Hosts	Any	HTTP	✓		Edit	Clone	Remove	☑	⇕ ➡
1	Hosts	Any	MAIL	✓		Edit	Clone	Remove	☑	⇕ ➡
1	Hosts	Any	HTTPS	✓		Edit	Clone	Remove	☑	⇕ ➡
1	Hosts	Any	SMTP	✓		Edit	Clone	Remove	☑	⇕ ➡
1	Hosts	Any	POP3	✓		Edit	Clone	Remove	☑	⇕ ➡

Graphic #6
(Allowed outgoing services graphic)

As we mentioned before, it is not a good idea to enable outgoing rules for services that are not strictly necessary, and if we have to, just enable in the rule the users or groups that are strictly necessary. This is why in our created rules we will only define the services exposed (Allowed outgoing services graphic). It is necessary to emphasize that we will not allow the access to Internet (i.e. navigation) directly from our servers because we can encounter a malicious code that can expose our servers. The updates and patches have to be analyzed before they were applied in our serves, that is because we can expose again our servers with default configurations. Finally, we will create a policy of access to our web server, with the mapping of the public IP in the external interface or Untrust of the firewall to a private and internal IP of our network[6] .

To do that we go to

Network→ Interface→ Untrust→ MIP→ New and create a MIP (mapped IP)



Graphic #7
Mapped IP configuration

[6] Netscreen Technologies, “Netscreen Concepts and examples Screen OS Reference guide Volume 2 Fundamentals”, URL: http://www.netscreen.com/services/support/product/downloads/screen_os/ce_v2.pdf (Chapter 4, Page 97)

In this part we set in the “Mapped IP” the public IP of our web server. In the mask, we leave the mask 255.255.255.255, this will guarantee a direct mapping from one to one IP and not to a subnet. In “Host IP Address” we place the private IP. Then we indicate in which virtual router it encounters. The virtual routers help us manage the protocols of the routing in the RIP and OSPF. The firewalls of Netscreen generally come with two virtual routers that can allow us to establish routing tables with different routing protocols such as RIP and OSPF, and separate one routing table for our internal network and the other routing table for our public network. In that way, we isolate both routing tables of our networks and get an extra security. What follows next, is how to allow the access from the exterior to the interior with access policy.

Policies–> From Untrust to Global

From Untrust To Global(MIP: X.X.X.X)

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
0	Any	WebServer	HTTP	✓		Edit	Clone	Remove	☑	
0	Any	WebServer	MAIL	✓		Edit	Clone	Remove	☑	
0	Any	WebServer	POP3	✓		Edit	Clone	Remove	☑	
0	Any	WebServer	HTTPS	✓		Edit	Clone	Remove	☑	

Graphic #8
Incoming rules permitted (access from the internet)

At this point, we should have already provided a certain degree of security to the “Developers” company, for the purpose of improve the configuration of security of the firewalls. We can configure the interface Untrust so that the web administration of the firewall can not be performed. Furthermore, we will take every possibility of management through Internet with options like SSH, by TELNET, SNMP, SSL, Ident-reset, NS-Global-PRO. A very important point is to try to avoid the firewall`s answer to an ECHO_REQUEST of ICMP taking off the PING option. As we know, a hacker starts his job of recognition through fingerprints that can generate the ICMP answer.
At this point, we have outgoing rules for the internal users and incoming rules for our server. At this point, we have already secured our network in a traditional way, but we have to add a configuration that can help us a little more with the security of our network.

Basic configuration of the IDS characteristics, personalized configuration for SOHO network

Now we enter into the most important part of our paper, which is to understand and personalize the basic IDS characteristics of the firewall.

It is well known that the majority of the intruders wish to prove their abilities or just satisfy their voyeur instincts. Those actions only leave tracks that represent lost of credibility or money to the company affected with these attacks. Therefore, within the basic IDS characteristics of Netscreen firewall, we can recognize some of the well known types of attacks from basic scanning up to denegation of service (DOS). The object of a denial of service attack is to disconnect the victim from the network or just a low performance. Several tools exist in the Internet in which much knowledge is not necessary to use them against the victim.
It exists several types of attacks protection; we will explain those as we advance in the customization of the firewall to our requirements. It is necessary to notice that the firewall in its basic IDS characteristics, does not only protect us against the attacks of the flood type as the majority of attacks DOS type. It also protects us blocking http components, defense of windows computers such us winnuke, defense against scanning and spoofing, predefined recognition of attacks of denial of service, detection of protocol anomalies in the IP layer and TCP/IP layer.
It is necessary to emphasize that for the example values that will be set in every option of protection of the firewall we will assume that we will have a small quantity concurrent users by (10 external and concurrent users per second). It is important to know how many users have access to our servers, which will help us to get our firewall fine tuned. It will also help us notice that the web page of the company does not have many components in its page. This is important because when performing the download of a page we can generate more than one session. Therefore, it is important that, at the moment of applying the values of protection, to have excellent knowledge of the load that have the servers which we are protecting, the quantity of users and a precise statistics of our servers.

Attack Protection[7]

Flood defense
ICPM Flood

This type of attack tries to consume the resources of the victim by sending an enormous quantity of ECHO_REQUEST. As the victim attends to all those petitions, reduces the performance of the victim to a point that the victim cannot receive more petitions even though those who belong or are made by a real and authentic user. To start our configuration we have to address the option menu.

Network→ Zones→ Untrust→ Edit→ Screen

In this first option, it is very important to configure the option of not disable it completely because it helps block unnecessary ICMP requests.
We have already disabled in Network→ Interface→ Untrust the option that allows the interface to answer to ICPM requests. However, we can enable this for our web server so that we can resolve the networking problems. The firewall comes configured by default with 1024 packets limit of ICPM Flood. If more than 1024 packets of this type reach the firewall, a drop will be made for each of those.

Now we can find a proper value for our fictional company. It is here where the considerations to the size of the company, the quantity of external concurrent users can be connected to the web server are made. Here is where our web statistics are used. Supposing that the statistics of web server never had more than 10 connections request per second; each of them thinks our server is shut down (when it is actually on and in production), the 10 users realize a ping to our server. Generally this is enough to know the delay in the four first packets with 32Bytes long each. Therefore, by calculating (10 users sending 4 packages of ICMP of 32 bytes by second by default in a normal ping) we have a value of 40 and it is not necessary to overload our server having to respond to 1024 packages by second. The value to which we will arrive depends of an analysis made previously to verify the requirements of the company. Therefore, we will place the value of 100pps (packets per second) in the ICPM Flood campus.

UDP Flood

Some applications such as the stream radio use UDP packages over the port 80 to transmit its contents. The policy of the company determines if it is necessary to enable a fair quantity of floods of UDP. So that our users do not feel bad about a moderate quantity of stream audio but we have to consider avoid attacks like TRINOO. Then we will make the necessary considerations taking in account that

[7] Netscreen Technologies, "INSG Course, Implementing Netscreen Security Gateways v4.0,", (April 2003). Networks Attacks, Appendix A.

we have 20 internal users. If there is a wish to listen to audio streams, we can configure these with a value of 300 packages per second. Each package posterior to 300 will be discarded and not taken into consideration by the firewall.

SYN Flood

It happens when a network becomes so overwhelmed by continuously petitions of TCP_SYNs to establish a TCP session and does not provide the correspondent ACK to complete the 3-way handshake of the TCP protocol. Therefore, it is necessary to know the type of server that we have and how much load it can support. If the amount of demand is not heavy; there is a needless expose of the server, so we can limit the amount of TCP_SYNs. As we said before we have our network statistic that says we have peaks with a maximum 10 users per second, considering that more than one of them can initiate more than one session for different reasons we can then limit the petitions to 5 per user per second. This is a reasonable quantity for the estimated load in the peak hours. Therefore, the value we can set in this session would be of 500 packets per second instead of 1024 packets per second that comes configured by default.

Alarm Threshold

In this option we have the limit of additional sessions, if together they overpass with the sessions of SYN flood they generate a register in the log of events with the degree of alarm. If they overpass the limited sessions of SYN that we have set, then the firewall will block the subsequent SYN packets. Therefore, the value that we can set here is 250pps (packets per second), this may increase to 7 or 8 user sessions and if the SYN packets reaches 751 (500 SYN + 250 Alarm threshold + 1 additional) it will be blocked.

Source Threshold

Most common attacks are recognized because the origin IP address generates too many requests for start a session; therefore it will depend on us the value that we recognize as an attack to the quantity of SYNs sent from one determined IP. It is necessary take in consideration at this point that an IP that generates too many SYN but can be one IP which is working with a proxy or one that works making NAT. The value by default is 1024 packets per second. We can reduce this to a minimum and arbitrary value of 300pps because maybe we can receive 300 SYN requests per second from one same IP, considering that it can be a team from a proxy or NAT is a considerable value.

Destination Threshold

As well as the protection that we set before we can limit in this case the SYNs which a destination IP address can receive. We have a web and mail services published in one server, so we must decide what value does not give our server a heavy load, therefore we set as an example a 500 SYNs packets per second, which could be a good choice for our web and mail server**.**

Time out

Usually this value is the amount of time that the firewall will wait for a packet. This value has to be in accordance with the performance of our network and the performance of our client's network which use our services. So if our network has a slower performance we have to increase this value, if not we can leave this value as default.

Queue Size

This value in Mb of the queue, will store the state of the connection or the necessary data, to detect an attack, for example to detect some fragmented attack, first the firewall will store all the fragmented packets, then it will rebuild the packet and check if it is not an attack. In this case, the firewall has another option, just block fragmented traffic, but it will depend of many facts such as network performance, type of traffic, etc.
Setting this value also will set an amount of memory to handle connections, such as numbers of session per source IP, then this queue value works together with the other options, and have to be a good size so we can set this value as default..

Blocking HTTP, Java, Zip y Exe components

Here we have the opportunity for blocking those types of components that usually comes through an http connection; it is up to us to set or not this option. In our case the company works in the development area, so it is common to receive those type of components so we choose not to block such components.
Also we have to keep in mind that so many codes and programs that arrive to our network have to be scanned for antivirus and malicious code.

MS-Windows Defense

This type of attack affect windows 95 and windows NT machines if they are not with the latest patch and service pack, this type of attack sends packets to our 139 port and we have not patched the computer's system which could crash or just disconnect from the internet. But in our case, we do not have computers with windows, so we choose not to activate this attack protection.

Scan / Spoof / Sweep Defense

IP Address Spoof

In this protection, first we have to know that a packet that comes from an interface associated to a segment network has a source IP from this segment, so if we find another source IP then we can say that is a spoof. It is a good idea to detect this because so many denial of service attacks use spoofing IP, and we do not want to be part of a DOS attack.

IP address sweep Protection

The Netscreen firewalls detect TCP scans but also can detect ICMP scans. The default value is 5000ms this means if more than 10 of our IPs are ICMP requested in less than 0.005 second, then an alarm is send. So keeping in mind that we have no more than 23 computers it is up to us to leave or change this value, thinking that we can set this value to 2000. So if we receive ICMP requests packets for more than 10 IP in less than 0.002 seconds the firewall will send an alarm[8].

Port Scan Attack Protection

This protects us against port scanning over TCP protocol. We have to know that it is in that way that an attacker could start a process to recognize the services in our servers, and could know what kind of software we are running on them. So if an attacker tries to make a scanning of 10 ports in less than 0.005 seconds the firewall will send an alarm, and if we want to be more paranoid we could set this value same as the sweep protection and set it to 2000; which means if an attacker tries to see if we have 10 open ports in less than 0.002 seconds the firewall will send an alarm[9].

[8] Sys-Security Group, Ofir Arkin "ICMP usage in scanning", (June 2001) http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf

[9] Insecure.org, Fyodor, The Art of Port Scanning, (September 6, 1997), http://www.insecure.org/nmap/nmap_doc.html , Scanning types

Denial of Service Defense
Ping of death Attack Protection

As we know the Ping Of Death is a type of a denial service attack, such attack tries to cut or slow down our connection sending an ICMP packet with a large amount of data in an ICMP request, so the victim if can not handle this packet just disconnects itself from the network, or maybe just slows down their performance. We do not want any of these, so it is important just to activate this protection, to prevent such attack[10].

Tear-Drop Attack Protection

The Teardrop Attack sends IP fragments to the victim but with modified offset values on each packet, so if the victim tries to reassemble these overlapped packets, it could cause a crash or in a windows system a blue screen. Also it is know that such attack in old kernel versions could crash Linux machines, anyway it is a good practice to activate this protection[11].

ICMP Fragment Protection

ICMP could help us to resolve networking problems and some times when we send an ICMP traffic through our network some network devices could cause an ICMP fragmentation, but just in some specific situations. Some hackers could use maybe like a reconnaissance method[12], we know that our network doesn't have many network devices so I think we can check this to protect a little more our network.

Large Size ICMP packet (Size > 1024) Protection

As it name says, this protection can help us to prevent receive packets with more than 1024 bytes size, for our little network. We do not need such packets, even if we have to solve some networking problems, in a large scale network. Maybe it will be necessary for a diagnostic problem or get some statistics.

Block Fragment Traffic

As I said before, some network devices could for many reasons fragment the packets to get through the network, is such cases before we activate this protection it is necessary for this and for all the protections to make a diagnostic for our network. Maybe activating a protection could cause an auto denial of service. The characteristics of the network of our example are simple, so we will not activate this protection.

---

[10] Insecure.org, Malachi Kenney, Ping of Death (October 21,1996), URL: http://www.insecure.org/sploits/ping-o-death.html.
[11] Hamburg Physics School, Security papers, Vulnerabilities URL: http://www.physnet.uni-hamburg.de/physnet/security/vulnerability/teardrop.html.
[12] Sys-Security Group, Ofir Arkin "ICMP usage in scanning", (June 2001) http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf

SYN-ACK-ACK Proxy Protection

This attack occurs when an attacker tries to connect to a service such as FTP or TELNET but does not complete the authentication, just initiates another session or many other sessions. This attack is similar to SYN flood but it takes place when the 3-way handshake ends and the attacker does not complete the login authentication. It is so important to maintain a session control, that way in a certain time we could have a lot of info that helps us to get some statistics or other valuable information. The default value is 512 for a single IP, we will reduce this for our example dramatically so we will set it for 50, because our services do not need to have an open session continually, and it is very rare that someone initiates more than 50 sessions from a single IP. Activating this protection could be a method to recognize an attacker.

Source IP Based Session Limit

This value represents the maximum sessions number that a source IP could have with our network, so the default value is 1024; keeping in mind that we have a SOHO network with not to much clients on our services. We can set here 128 sessions per source IP, which is an arbitrary value but a lower value, that must represent the study of your own network (how many clients, Branch offices, remotes offices) and how they connect to your headquarters.

Destination IP Based Session Limit

Same as before but here we can control how many sessions are permitted per destination IP, in that way it can be limited. The default value is 128 sessions. For our fictional network it is a good value, because we want to advertise our products, handle mail connections and this value is coherent with the others protections.

Protocol Anomaly Reports -- IP Option Anomalies

Here we can set the firewall to report us, protocol anomalies at layer 3 (IP) of the OSI model, many packets in their way to reach their destiny they pass through routers, switches, firewalls, etc. and maybe the packets could be modified to fit their way. In the other hand, some hackers use special and customized IP options to cause the protocol anomalies to try to find an exploit or some vulnerabilities on our devices. If we want to catch those anomalies to keep an eye in those packets, we can make an analysis to see if some sort of intrusion happened already. Therefore I think it is a good idea to check this option if we want to make a serious network administration.

Protocol Anomaly Reports -- TCP/IP Anomalies

As the precedent IP reports, we can receive reports if the firewall receive TCP/IP anomalies. As we already know, maybe some hackers use this anomalies to try to exploit some vulnerabilities so to remark it would be a good choice to set and receive a notification for all this anomalies.

Conclusion

At this time we have done helping our network administrator to secure their network. The firewall characteristics helps us to complete the task easily and shortly, the intuitive web interface of the firewall just requires from us a little knowledge of networking and with the help of this paper an administrator could reach their main objective which is to protect their network. Some values that we set could not be the optimal values but the values that we set in our own firewall have to be in accordance with the company policies and criteria.

It is very important to keep in mind that any security measure that we assume, needs to be started from a meticulous study of our company, and specifically with the firewall. If we need to create a rule, we need to know what objects we affect and how we will affect them. As we see for the Basic IDS configuration, we need to know what services are running or will run in the servers, what protocols, and how many users usually connect to them, etc. By this time, with the configuration made in the example, we have been able to keep our network a little secure. But some other things need to be considered such as: antivirus applications, maintain a study of the logs that our network devices generate and the log of our servers. As we see in these modern times, a firewall is not any more than what a firewall was years ago. So to choose a firewall it is a matter of planning, time, and resources. Therefore, we have to make a smart choice.
The basic IDS characteristics of the netscreen firewall does not replace an IDS itself, it just helps us a little in the boundaries of our network. Today more than ever, we have to use tools that help us to know what is going on in our networks.

So in this work I try to help how to configure and take advantage of the basic IDS characteristics in a Netscreen firewall. In a short time and serious way, this firewall has more options as others firewalls, but the Basic IDS characteristics were our main objectives.
And a thing to remark, no matter how many security devices and how good configured they are, we should improve the necessity in our users to protect their information. If they don't take care of their information our work will be insecure.

Reference

Netscreen Technologies, “Netscreen Concepts and examples Screen OS Reference guide Volume 1 Overview”, URL:http://www.netscreen.com/services/support/product/downloads/screen_os/ce_v1.pdf .

Netscreen Technologies, “Netscreen Concepts and examples Screen OS Reference guide Volume 2 Fundamentals”, URL: http://www.netscreen.com/services/support/product/downloads/screen_os/ce_v2.pdf Basic IDS options, page 33-43.

Netscreen Technologies, “Product Capacities Netscreen 5GT, Netscreen 5XT, Netscreen 5XP” URL:http://www.netscreen.com/products/at_a_glance/5xt_5xp.jsp

Netscreen Technologies, “INSG Course, Implementing Netscreen Security Gateways v4.0,”, (April 2003).

Netscreen Technologies, “NIDP Course, Netscreen Intrusion Detection and Prevention v2.0a2,”, (093-0724-000 2001).

Symantec Corporation, “Firewalls/VPN assegurando o perimetro” (Mayo 16,2001) URL:http://www.symantec.com/region/br/enterprisesecurity/content/content_firewall1.html.

Bastille-Linux, Jon Lasser - Lead Coordinator, The Bastille Hardening System attempts to "harden" or "tighten" Unix operating systems URL:http://www.bastille-linux.org/ .

Hamburg Physics School, Security papers, Vulnerabilities URL: http://www.physnet.uni-hamburg.de/physnet/security/vulnerability/teardrop.html.

Sys-Security Group, Ofir Arkin “ICMP usage in scanning”, (June 2001) http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf

Insecure.org, Fyodor, The Art of Port Scanning, (September 6, 1997) http://www.insecure.org/nmap/nmap_doc.html

Insecure.org, Malachi Kenney, Ping of Death (October 21,1996) http://www.insecure.org/sploits/ping-o-death.html.