GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Case Study: Deploying and Configuring a Netscreen 100 Firewall Appliance to Secure the Network

© SANS Institute 2003, Author retains full rights.

James M Murphy
GSEC: GIAC Security Essentials Certification
Version 1.4b
Option 2

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

I. Abstract 3
II. Before 4
III. During 5
A. Netscreen Firewall Products 5
B. Physical Device 5
C. Location of Device 5
D. Typical Network Configuration of an Organization 6
E. Configuration of a Netscreen Firewall 7
F. Upgrading the Netscreen Firmware 8
G. Setting the Systems' Clock 10
H. Setting Up Administrators 11
I. Securing Access to the Firewall by IP's 12
J. Secure Administration of Firewall 13
K. Security Warning Banner 14
L. Web Site Blocking 15
M. Log Configuration 16
N. Email Alerting 18
O. Configuring for Syslog 18
P. Using WebTrends with Netscreen 20
Q. Use of Netscreen's Global Pro/Express 21
R. DNS Configuration 22
S. Configuring the Netscreen Device for Attacks 23
T. Configuring the Interfaces of the Netscreen Device 25
U. Routing 25
V. Policies 26
W. Services 29
IV. After 32
References: 33

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

I. Abstract

Firewall implementation and deployments are done many times without much consideration or planning. Upper management in many organizations do not know what their firewall policies are, the type of firewall it is, or the configuration of the firewall. Often companies believe that firewalls are the magical silver bullet for their organization. It takes a lot to configure a firewall properly and to maintain it securely.

After being hired to take over Network Security responsibilities for my organization, I quickly realized that the deployment of our firewall architecture was flawed and the network was exposed due to the inadequate patch management of the NT operating system and the Checkpoint FW-1 application. After some analysis of the firewall architectures, senior management supported the decision to re-deploy a new firewall, architecture, and policies. The purpose of this document is to show the reader on how I deployed the Netscreen 100 firewall security appliance. It will also assist the reader in deploying and configuring a Netscreen 100 firewall via the command line (CLI) and the graphical user interface (GUI) and the reason why you should configure it using those options. The paper will focus on the firmware version 4.0 or higher.

This paper will follow the following conventions:

- CLI usages are set in *italic (e.g. set clock ntp).*
- GUI listings are set in **bold > (e.g. Configuration > Date/Time)** where Configuration > Date/Time are located in the left column of the browser.
- Instead of actual IP addresses, it is replaced with xxx.xxx.xxx.xxx. This will prevent current IP owners and production systems any negative exposure.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

II. Before

I was hired to administer the Network Security responsibilities of my employer in October 2001. I discovered quickly that the deployment of their firewall was in dire need of some immediate review. From a software/hardware level perspective it was buggy. The company was running Checkpoint FW-1 with no service packs even though at that time Service Pack 4 for Checkpoint FW-1 was already released. The application was running on NT 4.0 SP4 server. Since Service Pack 6a came out in December 1999, my employer was also way behind in applying patches to the operating system.

The NT server had three interface cards on the machine. One interface was to our Internet Service Provider's (ISP) external router, the second interface was connected to our internal router and the last interface was connected to our mail relay host, which was considered our DMZ (De-Militarized Zone). This configuration would have been good but unfortunately the company was providing services to the external network from our internal network using NAT (Network Address Resolution) and we had devices exposed to the external network in which no firewall was protecting the device. Our logs for Checkpoint were also on the same machine where the Firewall-1 application was installed. From a security viewpoint, this should have not happened. In the event our firewall was hacked, the logs could have been easily erased or modified.

The last major problem was the number of routes previous administrators had added. There were 30 routes added to the operating system. Many of these routes were unknown and nothing was documented to show why they were there in the first place.

There were also numerous best practices that should have been followed. Some examples were that the company did not restrict IP addresses to administer the firewall, offload logs to another server, no time synchronization, no logon banners, and so on.

The need was to immediately secure the current firewall or to recommend a new firewall architecture to senior management. One recommendation was to fix the current architecture, but the company would still have to address the process of applying patches to the operating system and to the application. The other recommendation was to replace the current architecture. We could use a network appliance that would have no operating system and just the firmware.

The final decision was made to migrate from an NT server running Checkpoint to a Netscreen appliance firewall. The ultimate reason for the migration to Netscreen was the use of a firewall appliance without an operating system and the tremendous reviews Netscreen had received from many trade groups.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

III. During

A. Netscreen Firewall Products

Netscreen firewalls are based upon on a stateful inspection technology. The Netscreen series of firewalls are hardware based firewall solutions. They are ICSA (International Computing Security Association) certified stateful inspection firewalls and IPSec VPN gateways. The Netscreen appliances have no operating system like NT/2000 or UNIX to operate. This helps reduces the risks to a firewall due to limitations of the operating system. It is utilizes a security ASIC (Application-Specific Integrated Circuit) which helps accelerates the firewall policy lookups and encryption and authentication algorithms within the hardware.

B. Physical Device

The three interfaces are labeled easily as "Trusted", "DMZ" and "Untrusted". The "Trusted" interface allows connections to an internal LAN. The "DMZ" interface allows for connection to a specific device within the DMZ such as a web server, a hub, or a switch. A hub connection broadcasts all traffic to all devices that are connected to a hub. A switch, a layer 2 or preferably a layer 3 switch, allows traffic to be sent to a specific device that a packet has been destined to go. "Layer 2 switches forward packets only by MAC address and ignore all higher layer aspects of a packet. Layer 3 switches forward packets based on Layer 3 protocols, such as an IP subnetwork or IPX network address.[1]" So depending on your security requirements, a Layer 3 switch may be a better solution.



There is a DB-25 serial connection that allows you to configure the Netscreen device locally. Also, there is a PCMCIA Memory card slot for additional storage of logs. Since the memory buffer can only hold so many log files they will get overwritten quickly. Depending on the number of logs so using a PCMCIA may be beneficial.

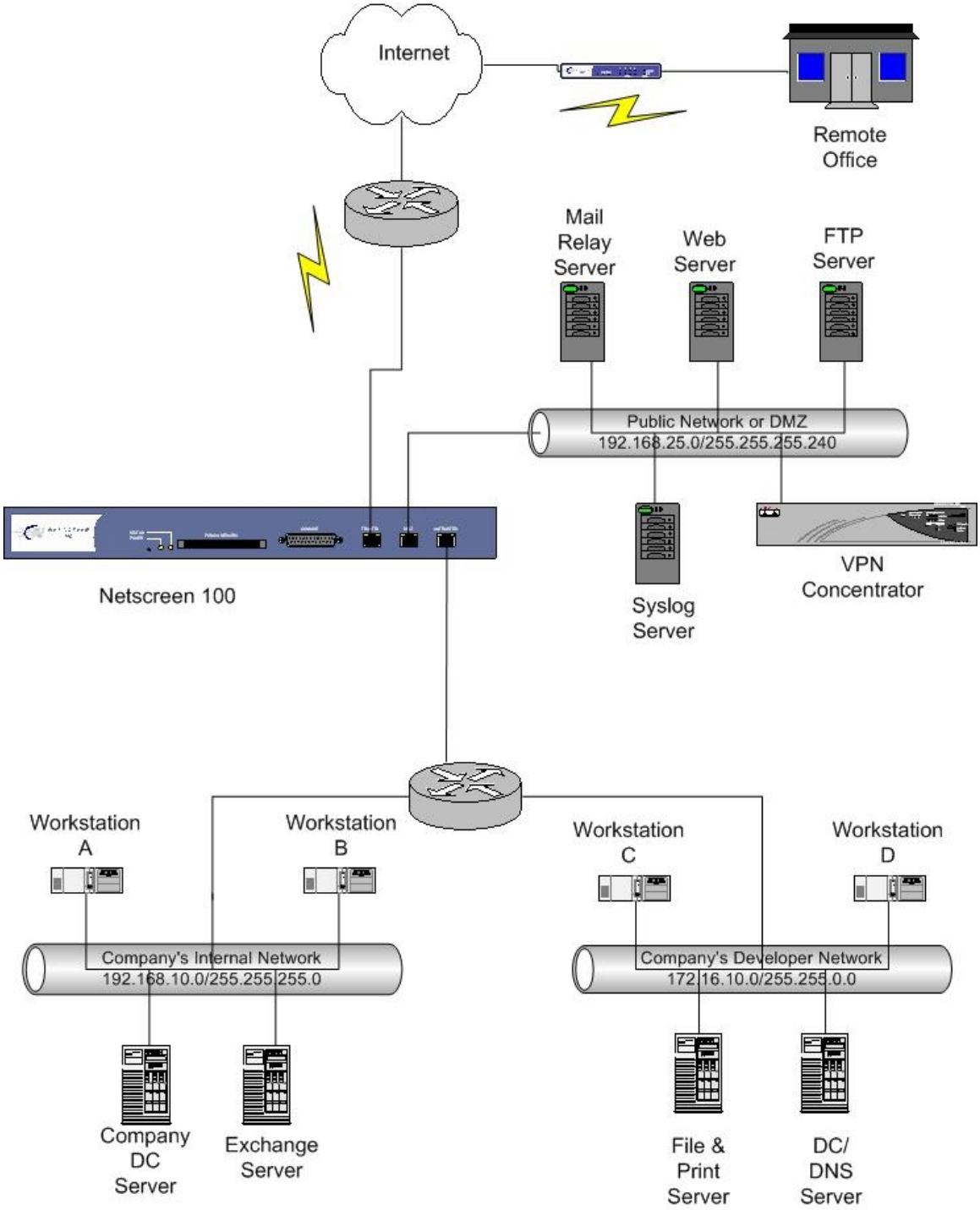
C. Location of Device

Where you place a Netscreen firewall is up to the decision of Senior Management and the firewall administrator. You may want have to have several firewalls throughout your network, but we will focus our attention on the entry point after the router which allows us to communicate to our ISP. This entry point will most likely separate the internal (trusted) network and the external (untrusted) network.

[1] Curtis, John and Andy Hacker, The many uses of the word "switching", http://www.nwfusion.com/newsletters/lans/0413lan2.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

D. Typical Network Configuration of an Organization



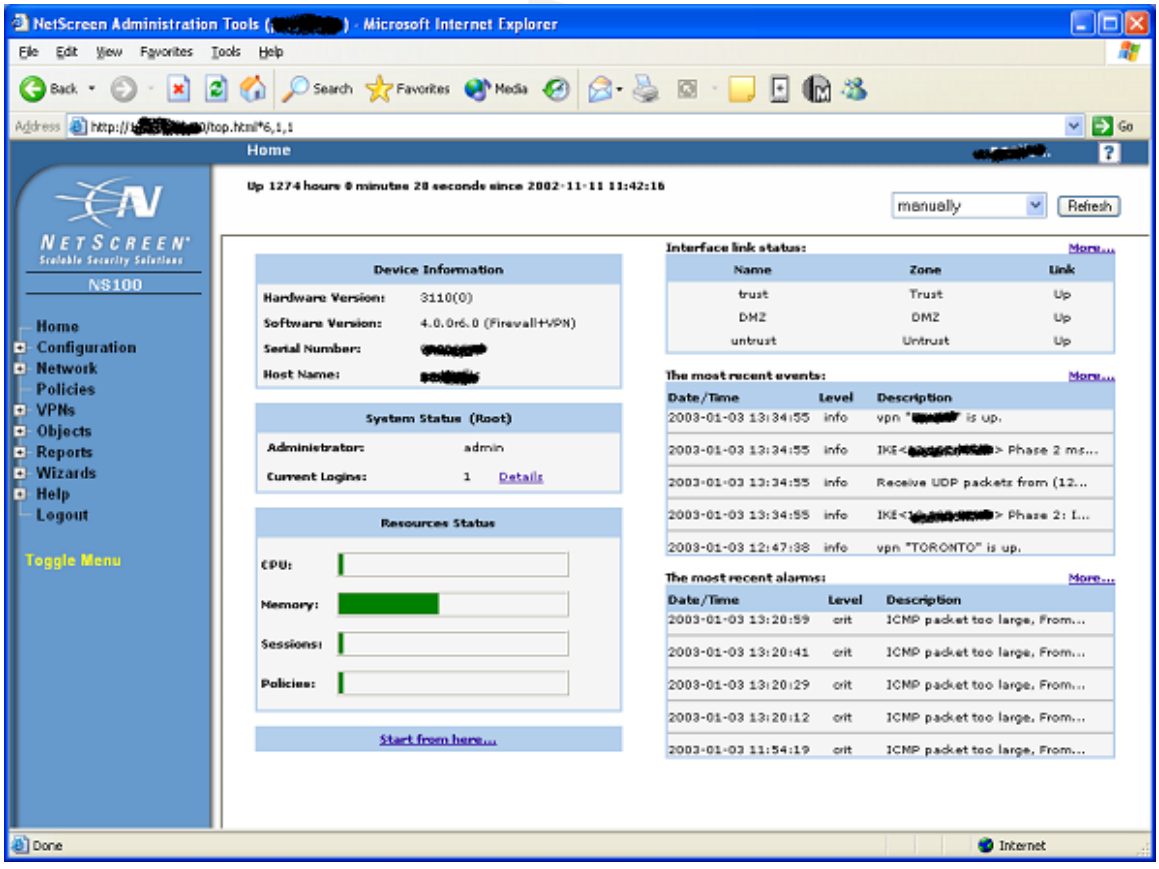
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In the previous diagram, we placed the Netscreen 100 firewall behind the outermost router. This router connects our ISP and our internal network. Since we had a web server, a mail server, and a VPN device, we wanted to place those devices within the DMZ. The rest of our systems would reside on our trusted network such as Domain Controllers and File & Print servers.

E. Configuration of a Netscreen Firewall

There are several options to configure a Netscreen firewall. The first option is via a DB-25 serial port connection that allows you to use the command line capability. This can be accomplished by using an application such as HyperTerminal. The second option is a GUI using your browser to configure the firewall through a network cable connection. Another option is to use Telnet or SSH (Secure Shell). This is also through the CLI. Some firewall administrators prefer to use the command line option because of its flexibility and capability to perform more tasks. It depends on your preference and your comfort level on which one is better. I will use both examples to help show the reader on how to configure the firewall via the command line and the GUI.

The following screen shot shows the GUI of a configured Netscreen firewall. The screen print indicates the Device Information, System Status, Resources Status, Interface Link Status, Most Recent Events, and the Most Recent Alarms. This information can also be obtained via the CLI. The graphical representation gives a quick status summary of the Netscreen device.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

F. Upgrading the Netscreen Firmware

When connecting to the firewall for the first time, the firewall was not connected to any other network. This allowed me to configure it off line. This prevented any unauthorized users trying to connect to the network before I had a chance to lock it down.

When you connect to the firewall via the default IP address as listed in Netscreen's documentation, one of the first things you want to do is to change the default user name and password from the vendor. For security purposes, I am not listing any vendor default user names, passwords, or IP addresses.

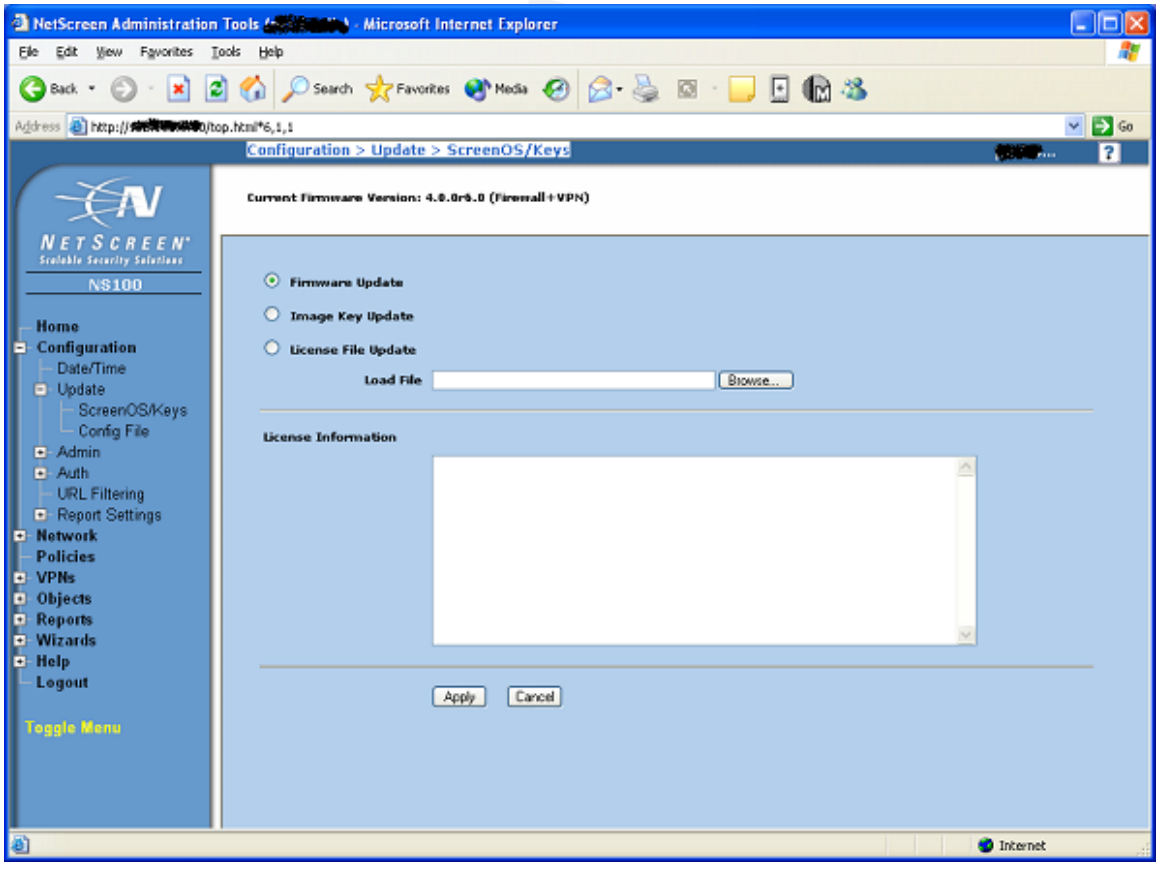
Since you are not connected to any networks, you need to copy these updates to your local machine to upload the latest release. These releases are posted at http://www.netscreen.com/support/current_release.html.

GUI

After downloading the firmware, you can upload the firmware by going to

Configuration > Update > ScreenOS/Keys

Select the "Firmware Update" radio button, select Browse, select the firmware and select "Apply". Upon completion of the update, the firewall will reboot itself.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

CLI

To update the firewall via the CLI, reboot the device. When you are requested, enter into the Boot Mode. The following is a direct knowledgebase article on how to update the Netscreen device via the CLI[2].

```
NetScreen Technologies Inc.
NS-5XP System Monitor V2.2
Copyright, 1997-2001

32M SDRAM detected
SDRAM test0 passed

AMD 29DL323DT

NetScreen Technologies, Inc
NS-5XP Load Software
Copyright, 1997-2001
Version 2.5

Hit any key for Boot/Diag mode

Hit any key for Boot mode
Hit any key for Boot mode

Serial Number  [0018062001002706]: READ ONLY
Control Number [00000000]: READ ONLY
HW Version Number [3010]: READ ONLY
Self MAC Address [0010.db0c.cbb0]: READ ONLY
Self IP Address [192.168.1.1]: 192.168.1.1<-- type IP address of trust
interface
TFTP IP Address [192.168.1.110]: 192.168.1.110<-- type IP address of
TFTP server
Boot File Name: [ns100.4.0.0r1] ns100.4.0.0r1  <-- type ScreenOS
filename
Save Boot Info (76) ... Done
tftp: load ns5xp.3.0.1r2.0 from 20.1.1.10
tftp malloc: 4f0c5c
rtatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatata
tatatatat
atatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatata
tatatatat
(omitted ...)
atatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatata
tatatatat
atatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatatata
tatatatat
atatatatatatatatatatatatatataTftp download complete (size = 1768506,
flash=0)!
********ignore image authentication!
platform = 10, cpu = 9, version = 16
offset = 20, address = 6d6000, size = 1768458
date = 0, time = 0, cksum = d9279538
```

[2] http://www.netscreen.com/support Solution ID: nskb606

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Program to flash (0)? y/[n] <-- enter "y"
Program flash (80000,1768506) ... ++++++++++++++++++++++++++Done
Run downloaded program? [y]/n <-- enter "y"
Start loading...
.............................................................
.............................................................
.............................................................
........................
Done.
```

G. Setting the Systems' Clock

One of the best things you can do for your network and logs is to have them synchronized with a common clock. The best way to accomplish this is to use Network Time Protocol (NTP). There are many public NTP servers available. There are two types of NTP Servers – Stratum 1 or Stratum 2. Stratum 1 servers are primary NTP servers and Stratum 2 servers are secondary servers. Please check the restrictions for each server before connecting to it. I selected a Stratum 1 server from the University of Massachusetts. You may want to select other servers from different areas of the world for failover scenarios.

http://www.eecis.udel.edu/~mills/ntp/servers.html

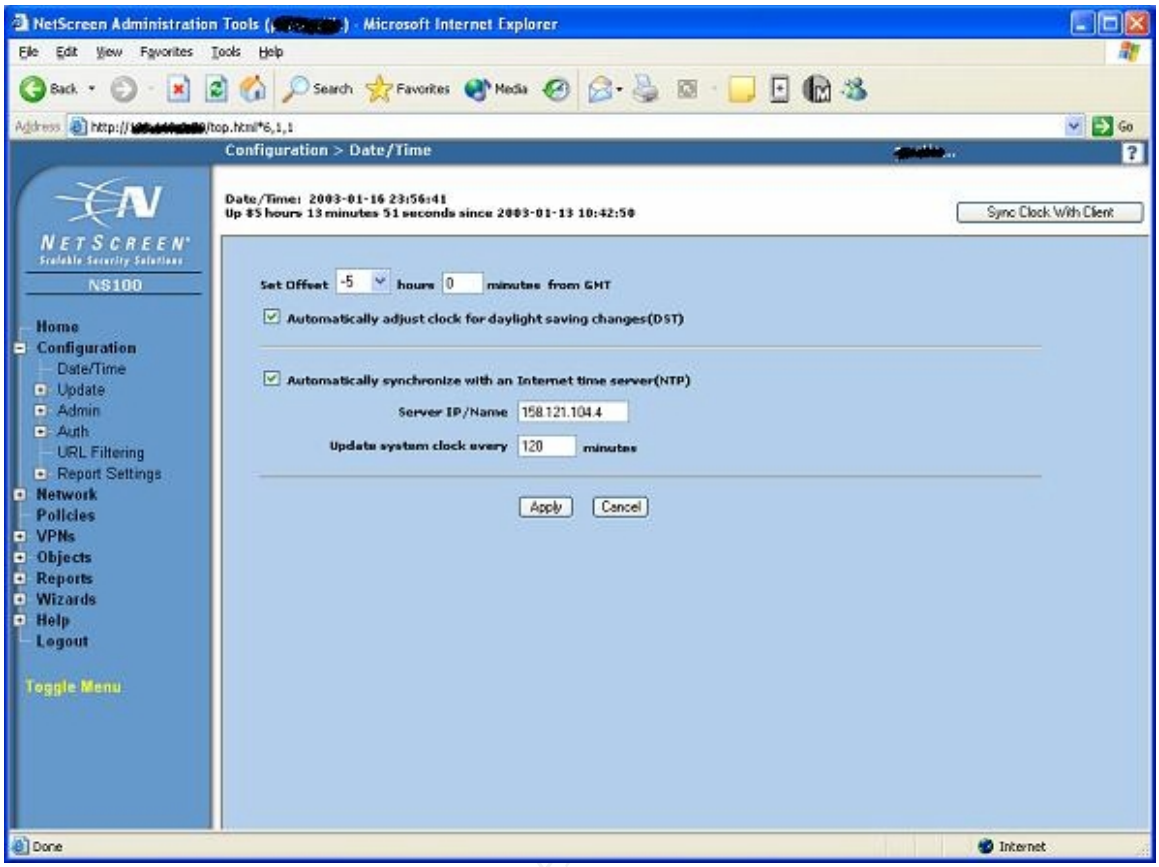
GUI

Configuration > Date & Time

Within this view, you can select "Automatically adjust clock for daylight savings changes (DST)" to adjust for DST. To synchronize with a NTP server, select "Automatically synchronize with an Internet Time Server (NTP)". Enter the IP address in the "Server IP/Name" field and select the "Update System Clock every x minutes" and select a refresh variable and then select "Apply".

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



CLI

set clock ntp
set clock "timezone" –5
set ntp server 158.121.104.4
set ntp interval 120

H. Setting Up Administrators

As mentioned before, one of the first things I did was changed the default user name and password from the vendor. After you rename the "root" account, you also may want to add additional administrators as required, up to five administrators on a Netscreen 100. You may select those administrators to have all access or read only. If in the event you have an auditor or an outside consultant to review your configuration you may want to give that user read only capability so that they can review your configuration. In my organization, no one uses the "root" account unless it's needed. However, there are several security personnel who have "All" access.

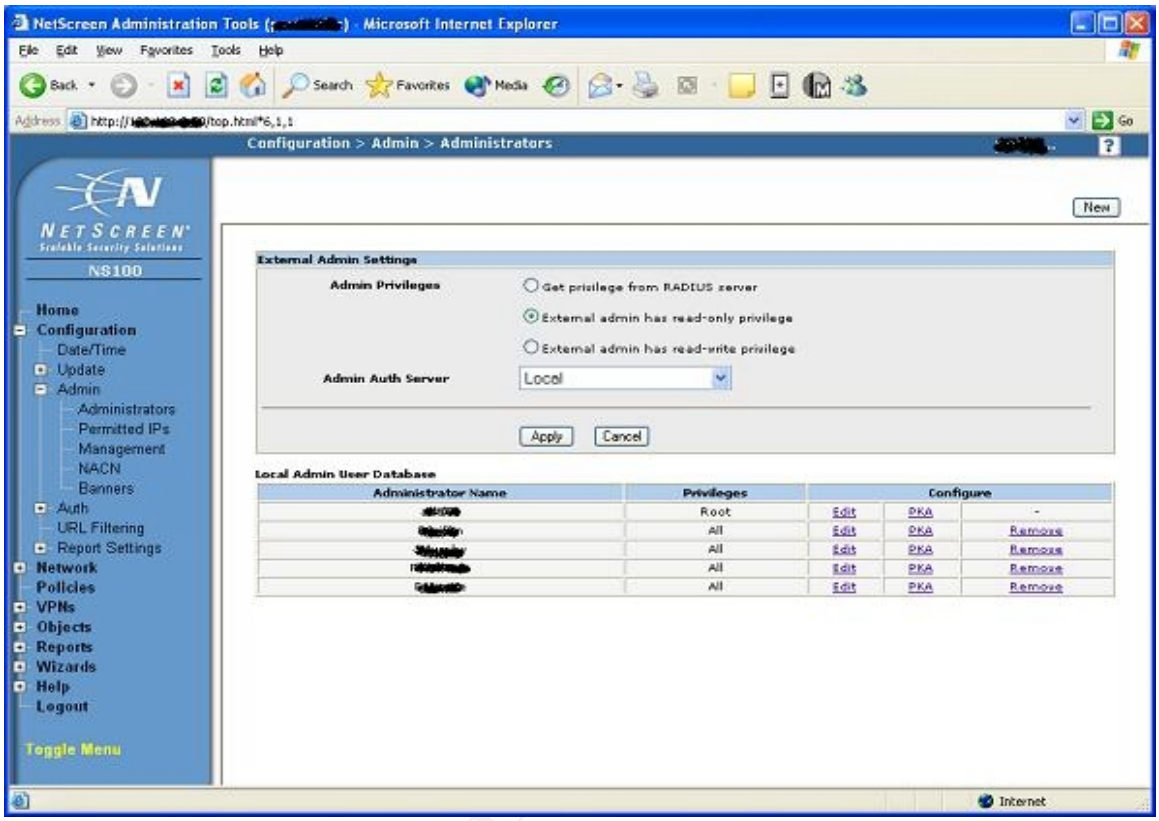
GUI

Configuration > Admin > Administration

The "root" account was renamed by selecting edit per the change control procedures. To add a new administrator, select the "New" icon and a secondary screen will appear. Enter the new administrators "Name" and have them enter their choice of a password,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and which type of access they will have – All or Read-Only. Again, once completed, select "Apply".



CLI

set admin format dos
set admin name "admin"
set admin password nH51EerE6zhNcLo26t3b9KpZCtpoCsCn
set admin user "JMurphy" password "nHVLHDrSFo26t3c8lJrsjITVGtOgBdun" privilege "all"

I. Securing Access to the Firewall by IP's

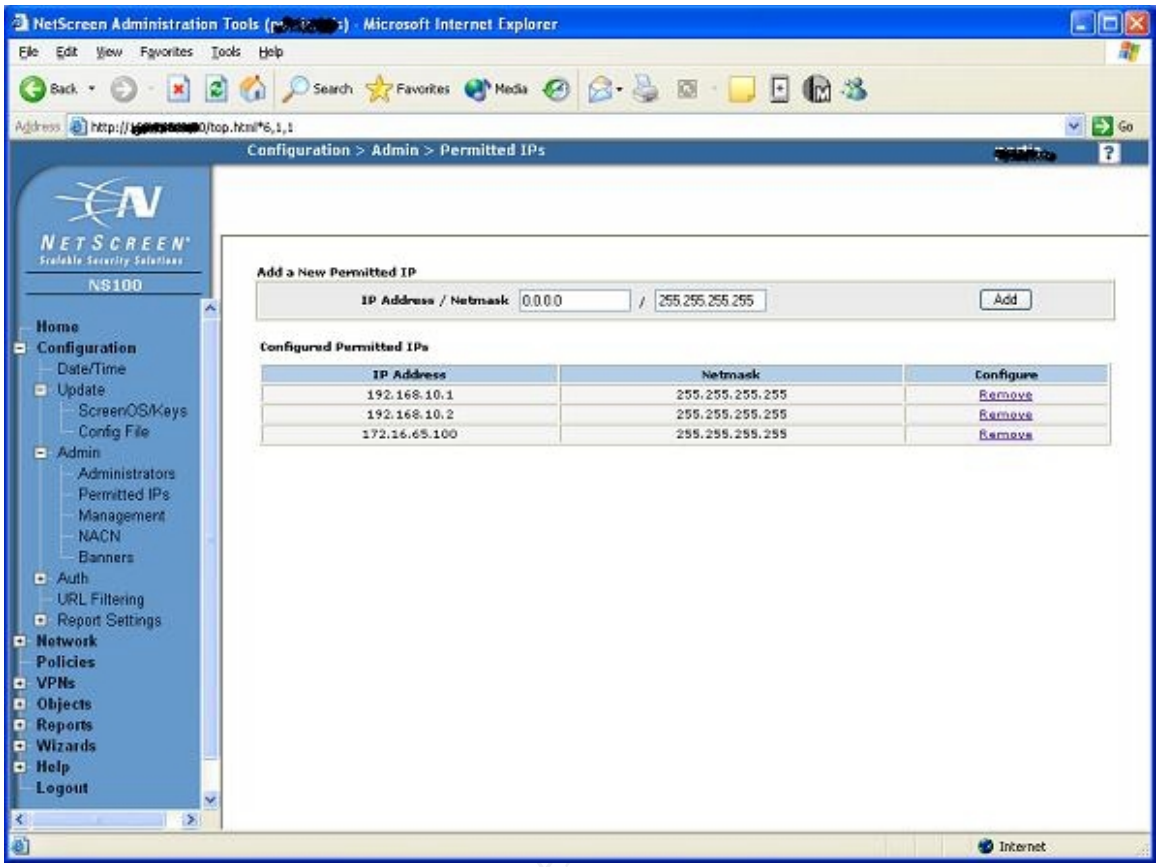
Restrictions were put in place for who could administer the firewall. This can be accomplished by allowing only a specific IP address or a range of IP Address of up to six IP addresses to manage the firewall. In this example I am allowing only 172.16.65.100, 192.168.10.1, and 192.168.10.2.

GUI

Configuration > Admin > Permitted IP's

Select the "Add" button and within the "Add a New Permitted IP" enter the specific IP address or range (and proper subnet) in the IP address and Netmask fields.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



CLI

set admin manager-ip 172.16.65.100 255.255.255.255
set admin manager-ip 192.168.10.1 255.255.255.255
set admin manager-ip 192.168.10.2 255.255.255.255

J. Secure Administration of Firewall

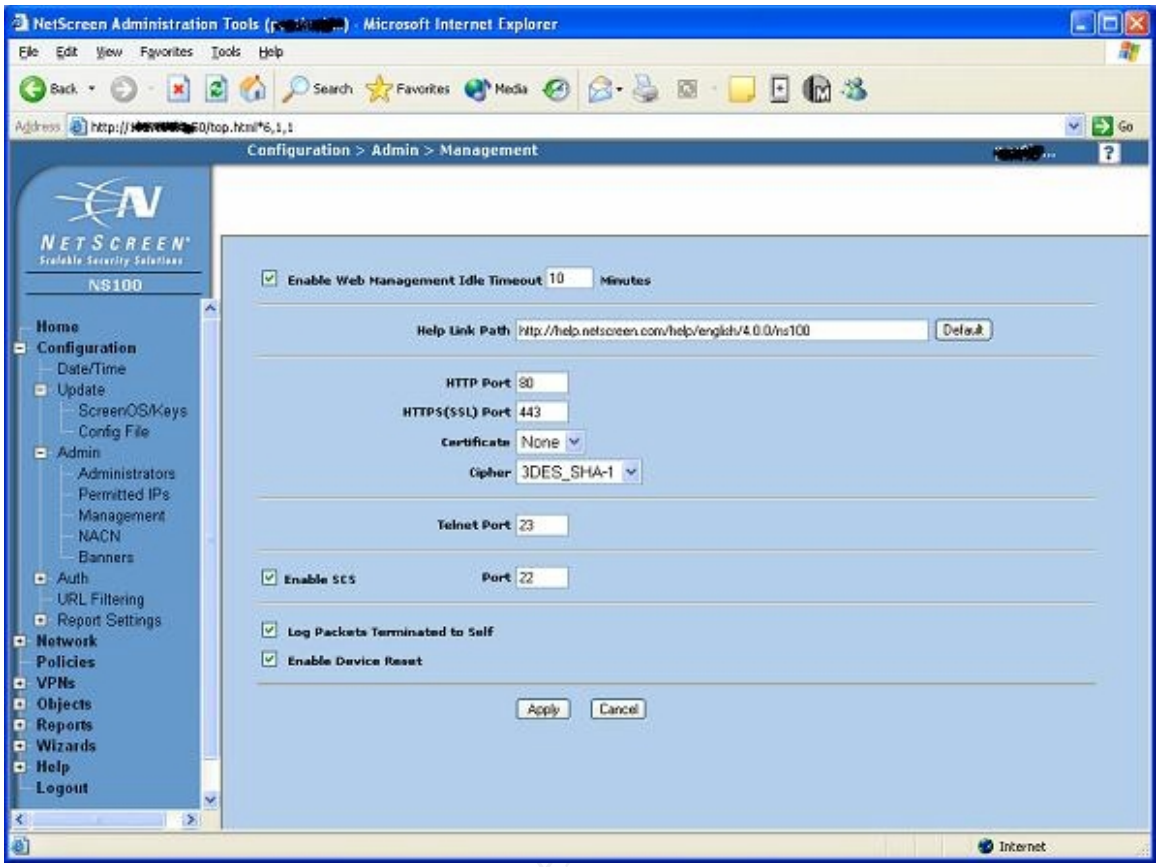
The Netscreen 100 device was configured to administer the device using encryption. The firewall can be managed securely through the console, https (port 443), and SSH (port 22) or it can be managed insecurely through http (port 80) or telnet (port 23). The option to select a security timeout feature administration is available. Management of the firewall is also available through Netscreen's Global Pro or Global Pro Express.

GUI

Configuration > Admin > Management

Select "Enable Web Management Idle Timeout" for the timeout feature for Administration, select "Enable SCS" for Secure Shell, select "Log Packets Terminated to Self" for packets that are dropped, and select "Enable Device Reset" for resetting the device by unsetting all options via the CLI. Usually the default information is fine unless you would like to change it manually for example to use a different port number for SSL. Once completed select "Apply."

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



CLI

set scs enable
set admin auth timeout 10
set admin auth server "Local"
set ssl encrypt 3des sha-1

K. Security Warning Banner

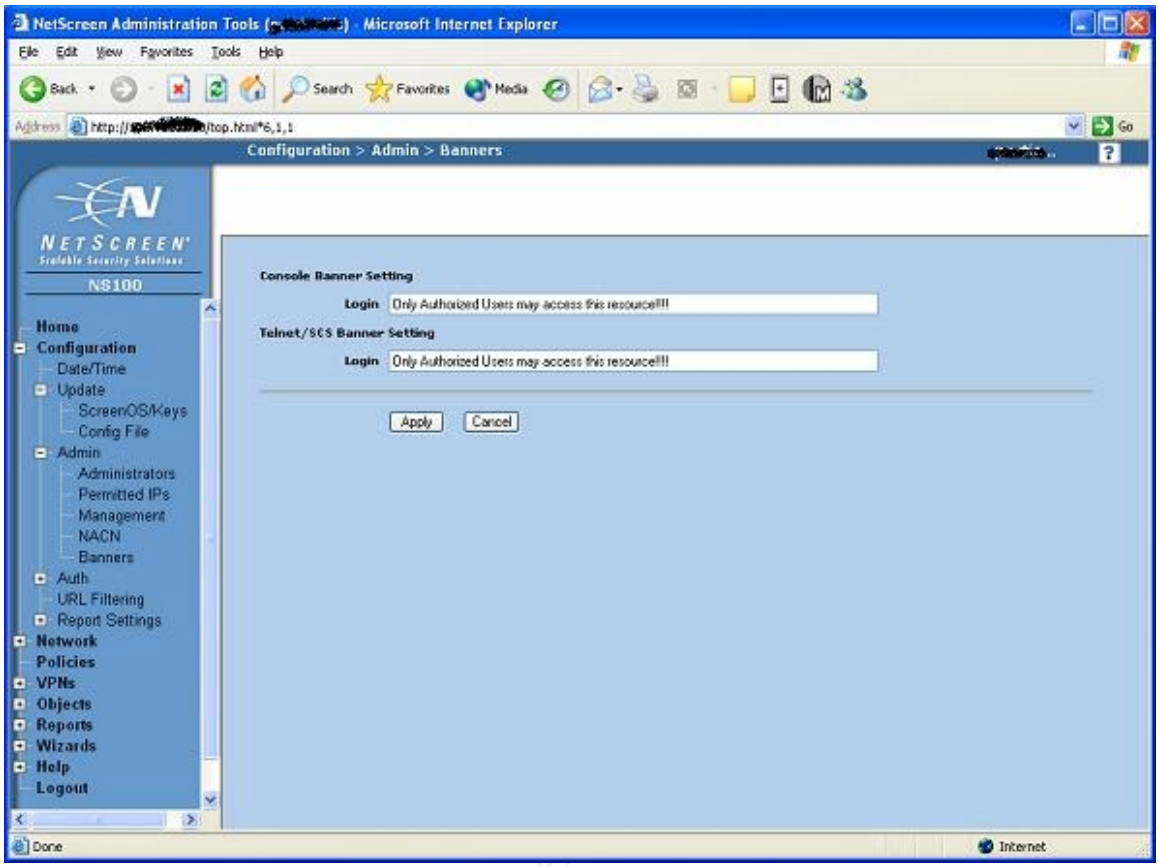
Depending on your company's security policy, you may need to add a warning banner upon logon. It was agreed that my organization would follow this practice and I added the banner language to the firewall.

GUI

Configuration > Admin > Banners

Within each "Login" field, enter the text you want to broadcast when administrators attempt to login and select "Apply".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



CLI

set admin auth banner telnet login "Only Authorized Users may access this resource!!!!"
set admin auth banner console login "Only Authorized Users may access this resource!!!!"

L. Web Site Blocking

The firewall was configured to block inappropriate sites by purchasing software from Netscreen's partner Websense. They have software that blocks access to inappropriate sites based upon your company's policy. It uses port 15868 by default and reconnects every 10 minutes by default for new updates to its database.

http://www.websense.com

GUI

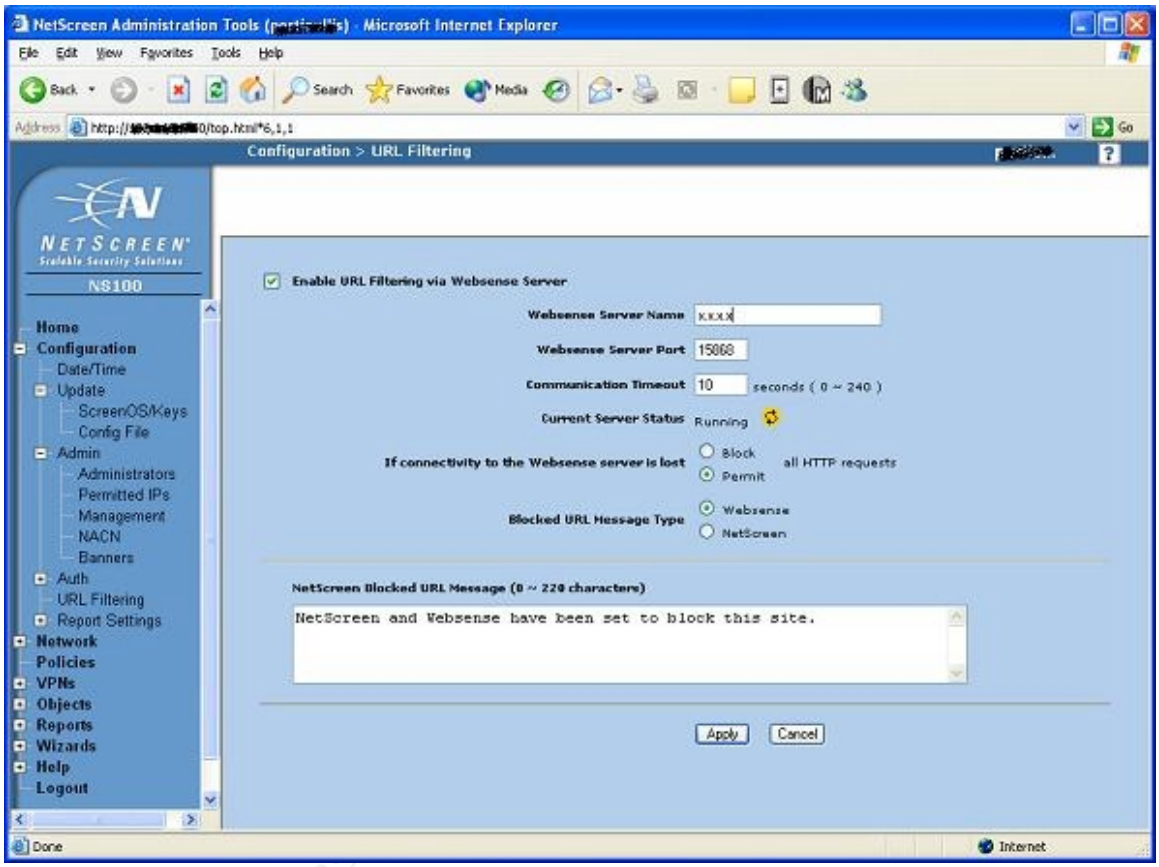
Configuration > URL Filtering

Select the check box for "Enable URL Filtering via Websense Server" to enable the use of Websense. Enter the IP address within the "Websense Server Name" field. Usually the default port, 15868, is the one you want to use unless you manually want to change it on the Websense server. Select the option "If connectivity to the Websense server is lost" to "Block" or "Permit" depending on your needs. If the connection to the Websense server is lost, you can deny all web access. That policy would notify you quickly because

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the users in your organization will be complaining of no web access. However you may also receive a phone call during off hours because of no web access. Is this the support you want to provide? I would recommend selecting the "Permit" option and use another means, like SNMP, to monitor the server. Even temporary access to inappropriate sites may be a legal issue that your organization's lawyer should address. You can also select which message to display when a user attempts to get to inappropriate site – Websense or Netscreen. When completed, select the "Apply" button.

.



CLI

set url server <xxx.xxx.xxx.xxx> 15868 10
set url fail-mode permit
set url config enable

M. Log Configuration

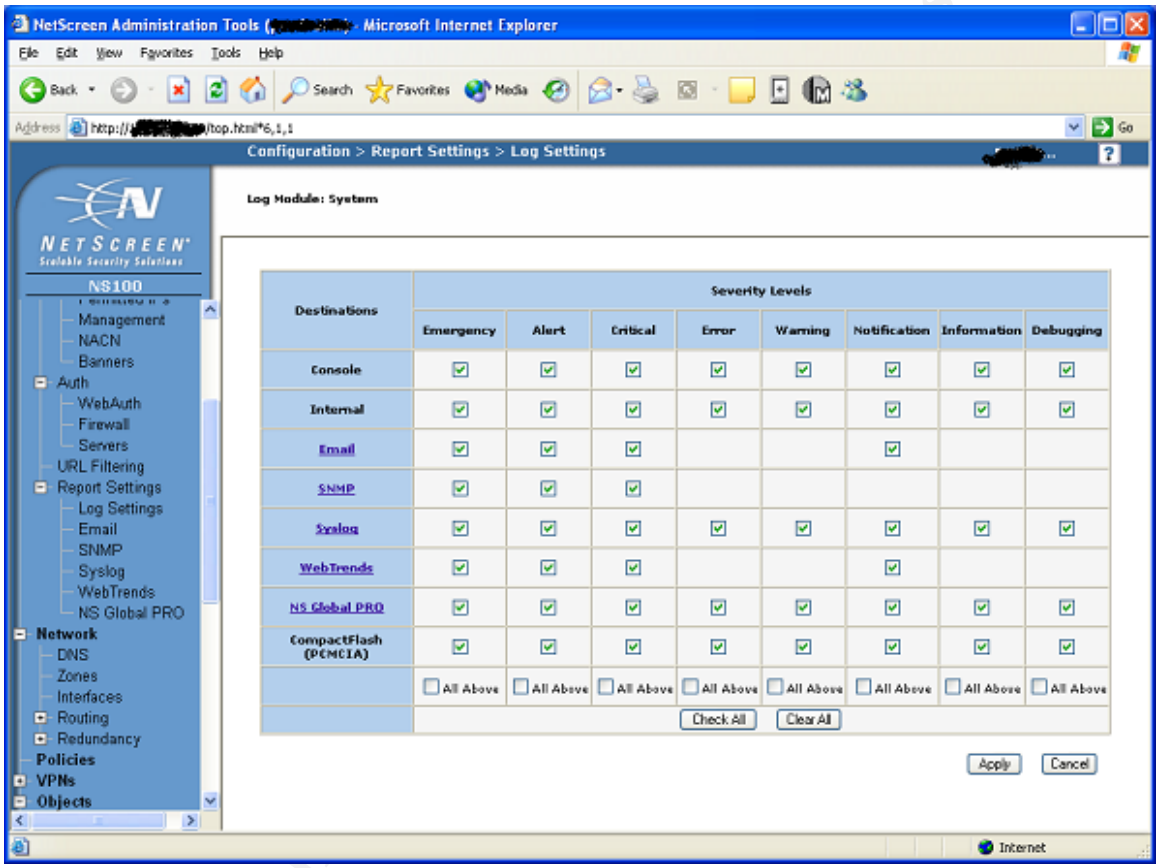
Depending on how useful logs may be to your organization, you may want to enable all logging for analysis and troubleshooting. I would recommend investing in a Syslog server. This can be accomplished through a UNIX server running a Syslog daemon, Windows using a third party product like WebTrends from NetIQ or a freeware product like Kiwi or WinSyslog. I recommended to our management team to use Kiwi's Syslog. It was robust enough to handle our log activities. This application can be installed on a Windows 2000 server, which my management appreciated instead of using a Unix server where there was a lack of knowledge on how to administer a Unix server properly.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The following screen shot indicates the security levels you can select for each type of destinations like E-Mail, SNMP, and Syslog.

GUI
Configuration > Reports > Log Settings

Select “Check All” and then select “Apply”



CLI
set log module system level emergency destination console
set log module system level critical destination console
unset log module system level emergency destination onesecure
unset log module system level alert destination onesecure
unset log module system level critical destination onesecure
unset log module system level error destination onesecure
unset log module system level warning destination onesecure
unset log module system level notification destination onesecure
unset log module system level information destination onesecure
unset log module system level debugging destination onesecure

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

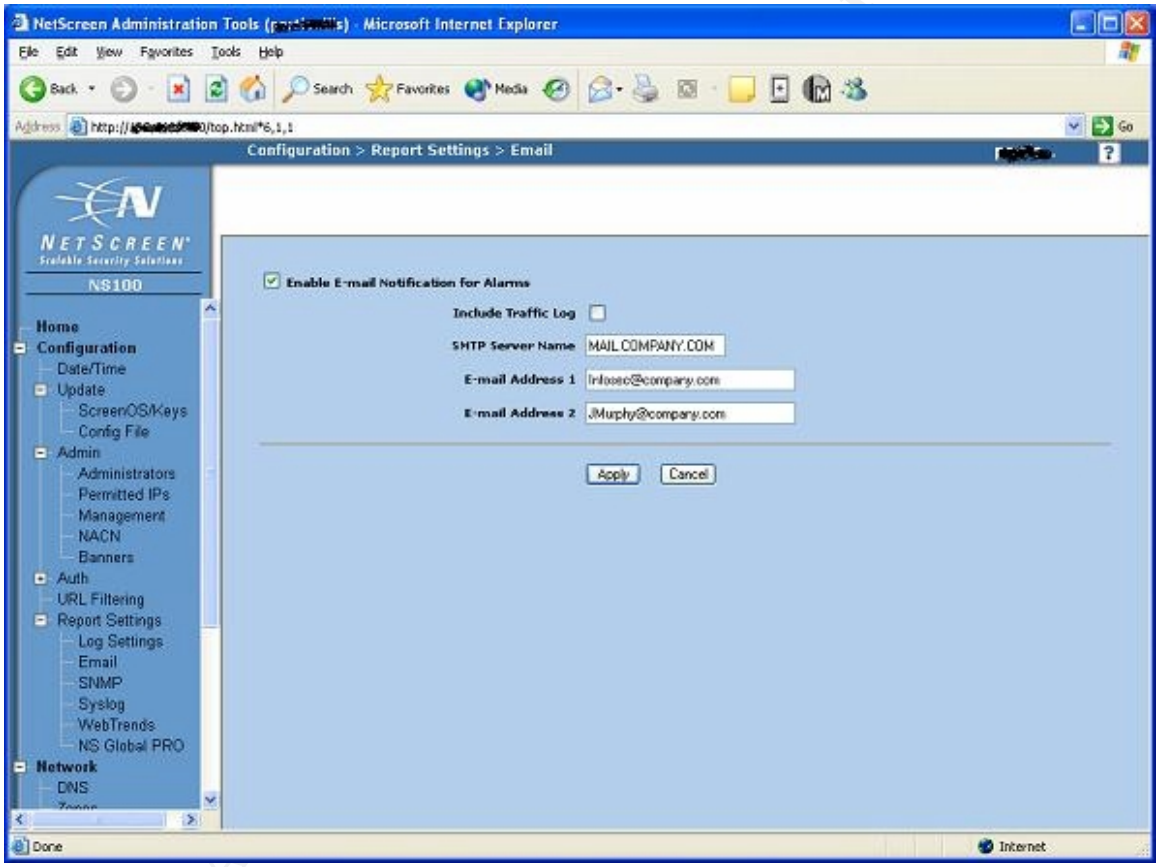
N. Email Alerting

To send email alerts of up to two addresses, configure your firewall for a mail server and two addresses. There is an option to send traffic logs via email but I choose not to do so because of the information being sent is in clear text through SMTP.

GUI

Configuration > Reports > Email

Check "Enable E-Mail Notifications for Alarms" and enter the name of your SMTP server for the "SMTP Server Name" field. Enter the email address you would like to use with the "E-Mail Address" fields. Again, once completed, select "Apply".



.

CLI

set admin mail alert
set admin mail server-name mail.company.com
set admin mail mail-addr1 Infosec@company.com
set admin mail mail-addr2 JMurphy@company.com

O. Configuring for Syslog

As mentioned previously, this can be accomplished through a UNIX server running a Syslog daemon or Windows using a third party product like WebTrends from NetIQ,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

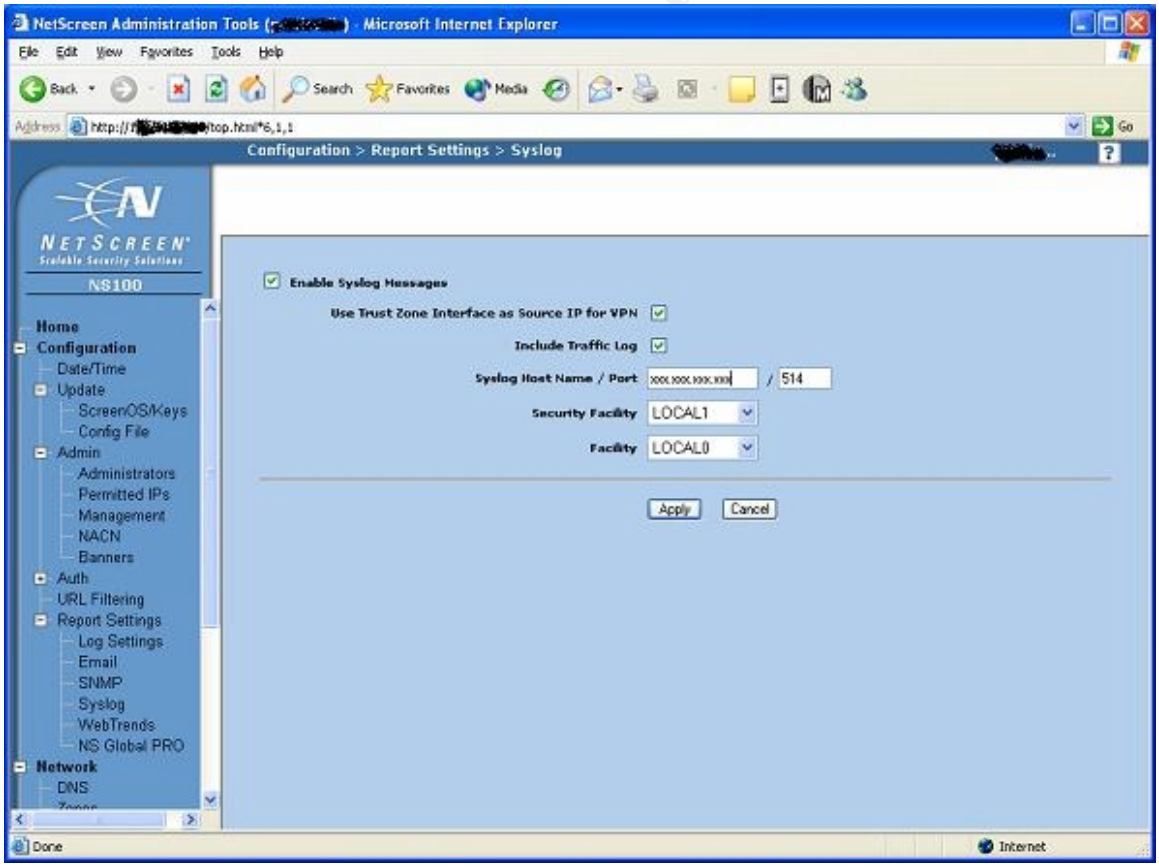
freeware like Kiwi or WinSyslog, or Netscreen's Global Pro. Syslog really should be used to store all the logs within your network on this server. It should only have Read-Only access**.** I installed Kiwi Syslog on a Windows 2000 server on a different trusted network. This server was a stand-alone server and only a few security devices and administrators could access the server.

GUI

Configuration > Reports > Syslog

Check "Enable Syslog Messages" to enable Syslog, "Use Trust Interface as Source IP for VPN" to send Syslog messages through a VPN tunnel, and "Include Traffic Log" to send your traffic logs to your Syslog server.

Enter the IP address of your Syslog server in the "Syslog Host Name" field and keep port 514 as the default. The defaults for "Security Facility" and "Facility" are usually the best option unless your organization has different needs. As always, when completed, select "Apply".



CLI

set syslog config xxx.xxx.xxx.xxx local1 local0 debug
set syslog enable

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

set syslog traffic
set syslog VPN

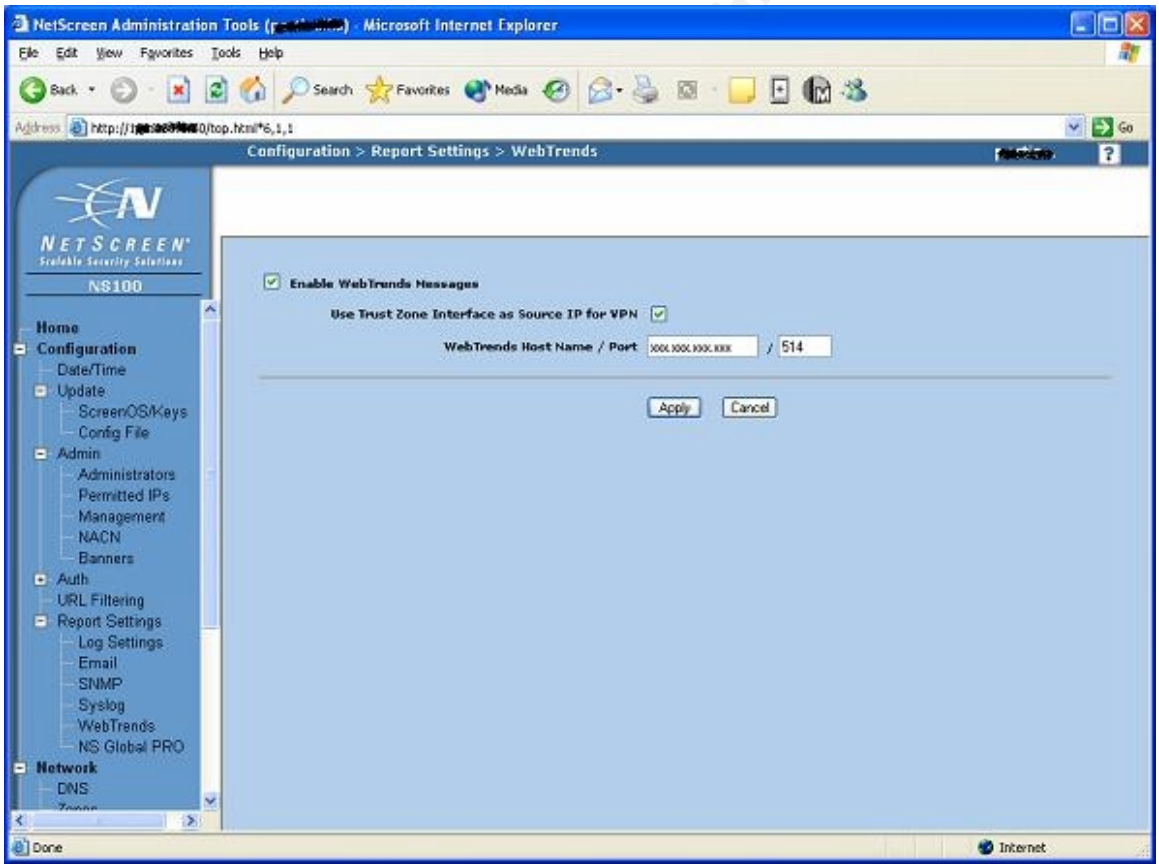
P. Using WebTrends with Netscreen

We decided to use Net IQ's WebTrends who partners with Netscreen. Their product, WebTrends, can be used to analyze and monitor your firewall and VPN connections. In order to use WebTrends the following needs to be configured.

GUI

Configuration > Reports > WebTrends

Select "Enable Web Trends Messages" to enable the use of Web Trends and select "Use Trust Zone Interface as Source IP for VPN" to enable the use of a VPN tunnel for secure transmissions of Web Trends messages. Enter the IP address for the "Web Trends Host Name" field, keep the default port of 514, and select "Apply" when completed.



CLI

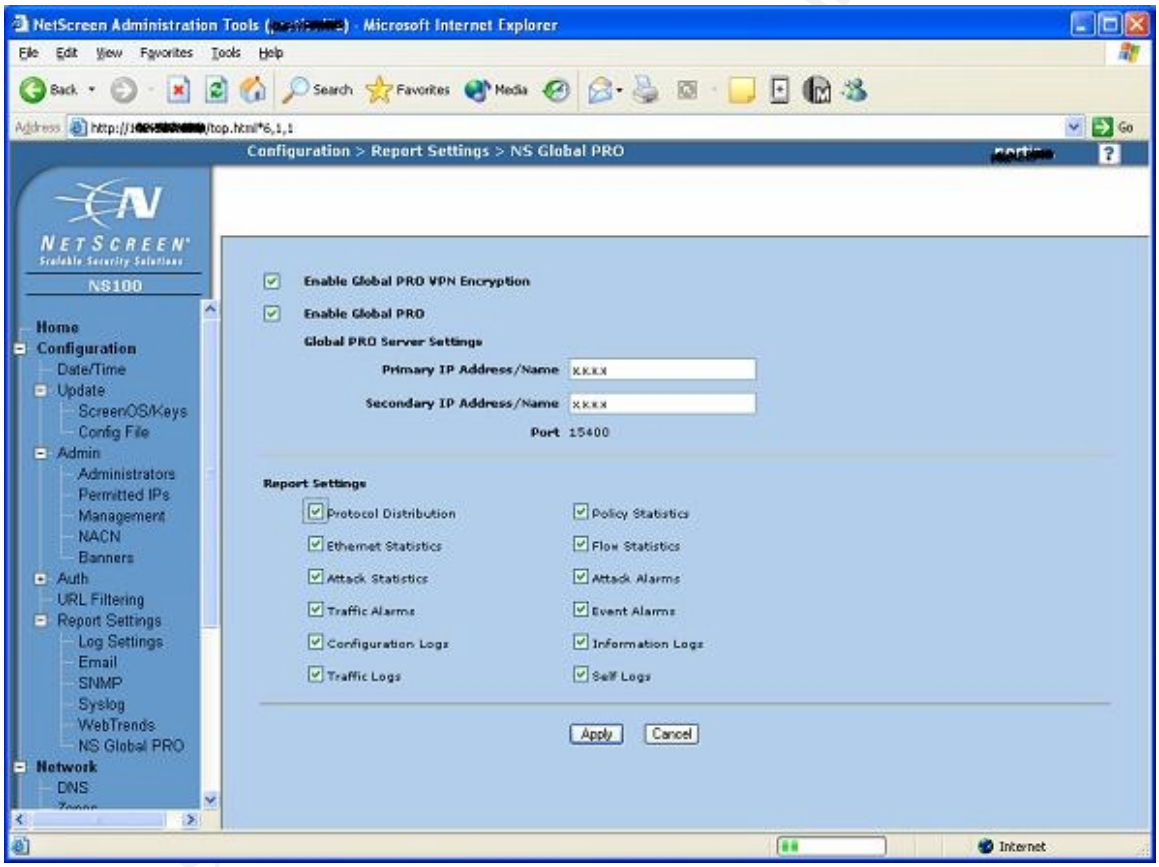
set webtrends enable
set webtrends host-name xxx.xxx.xxx.xxx
set webtrends port 514
set webtrends vpn

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Q. Use of Netscreen's Global Pro/Express
The company chose to use Global Pro Express because of the number of firewalls and VPN's we were administering. This product can manage many firewall appliances from a single location and all system configurations can be seen from a single location.

GUI
Configuration > Reports > NS Global Pro

To enable the use of Global Pro, check the "Enable Global Pro" and check the "Enable Global Pro VPN Encryption" for the use of encryption. In the "Primary" and "Secondary IP address" fields, enter the IP address of the Global pro servers. Select the "Report Settings" you wish to enable if not all. Once completed, select "Apply".



CLI
set global-pro report proto-dist enable
set global-pro report ethernet-stat enable
set global-pro report attack-stat enable
set global-pro report flow-stat enable
set global-pro report policy-stat enable
set global-pro report alarm-traffic enable
set global-pro report alarm-attack enable
set global-pro report alarm-other enable

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

set global-pro report log-config enable
set global-pro report log-info enable
set global-pro report log-self enable
set global-pro report log-traffic enable
set global-pro policy-manager primary outgoing-interface untrust
set global-pro policy-manager secondary outgoing-interface untrust

R. DNS Configuration

Depending on your situation, you may want to use internal or external DNS for resolution. If you have an internal DNS server, you may want to list your internal DNS servers on your firewall to resolve address by name instead of IP especially if you use DHCP. You can however have your external DNS be listed so users may resolve to the Internet if there is no internal DNS. In my organization we use DHCP. I decided to use internal DNS to resolve the host names instead of changing the IP addresses of those hosts within the firewall.

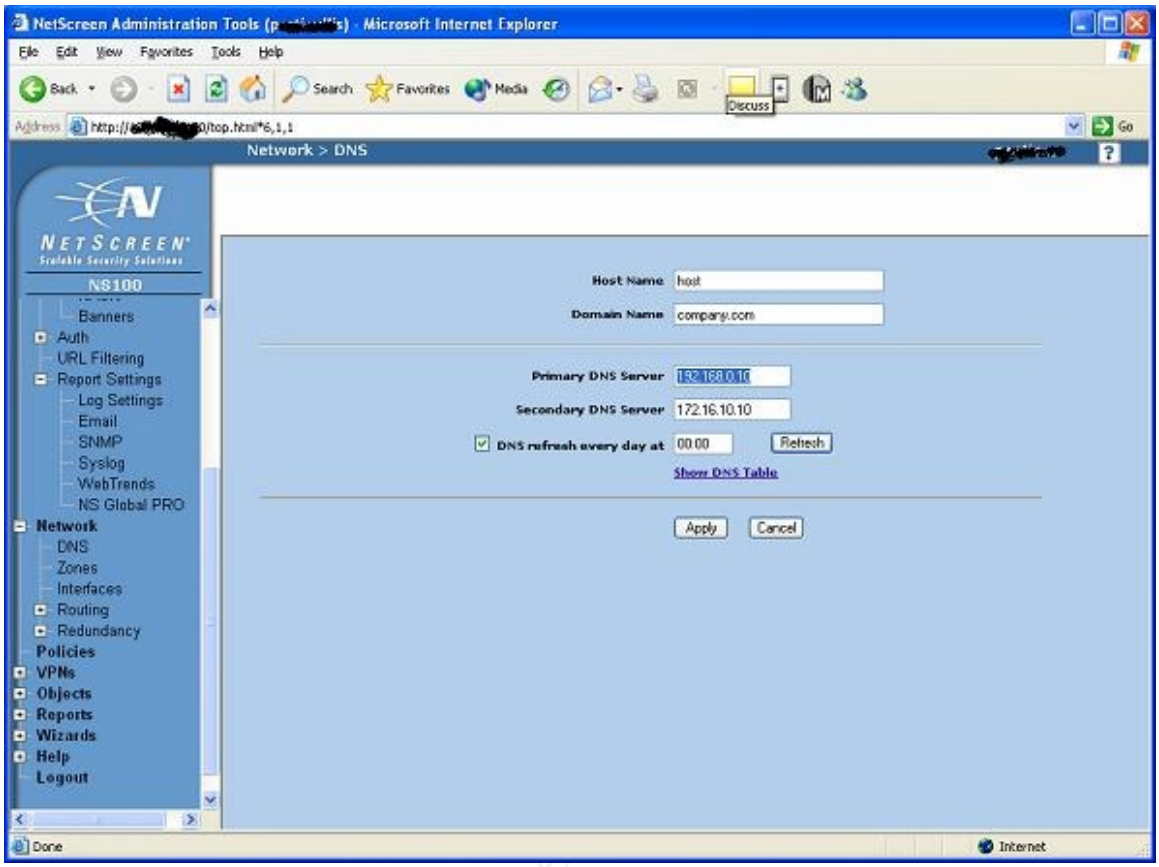
GUI

Network > DNS

Enter the host name within the "Host Name" field and your company's domain within the "Domain Name" field. Enter the "primary" and "Secondary DNS Server" IP addresses in the fields provided and select "DNS refresh every day at" to enable automatic refresh of the DNS tables daily at the time you specify. Again, once completed, select "Apply".

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



CLI

set dns host dns1 xxx.xxx.xxx.xxx
set dns host dns2 xxx.xxx.xxx.xxx
set dns host schedule 00:00

S. Configuring the Netscreen Device for Attacks

Each Zone or Interface has the capability to detect attacks such as syn-floods, ip-spoofing, Win nuke, and a lot more. We decided at first to turn on all options and review logs regularly. This will help us understand what is happening to our firewall and/or network.

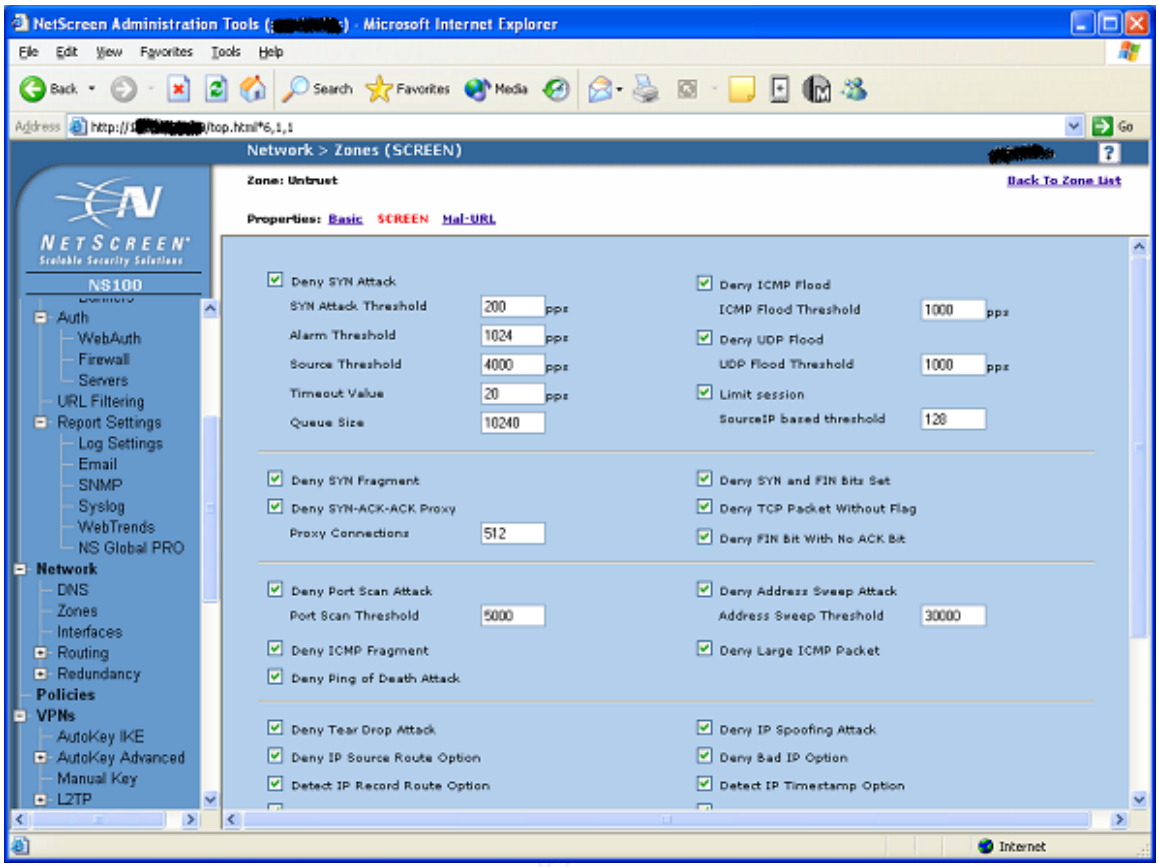
This screen shot shows the untrusted zone having all options selected.

GUI

Network > Zones

Select all options and use the defaults given and select "Apply". Over time you may want to tweak those settings.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



CLI

set zone Untrust screen icmp-flood
set zone Untrust screen udp-flood
set zone Untrust screen winnuke
set zone Untrust screen port-scan
set zone Untrust screen ip-sweep
set zone Untrust screen tear-drop
set zone Untrust screen syn-flood
set zone Untrust screen ip-spoofing
set zone Untrust screen ping-death
set zone Untrust screen ip-filter-src
set zone Untrust screen land
set zone Untrust screen syn-frag
set zone Untrust screen tcp-no-flag
set zone Untrust screen unknown-protocol
set zone Untrust screen ip-bad-option
set zone Untrust screen ip-record-route
set zone Untrust screen ip-timestamp-opt
set zone Untrust screen ip-security-opt
set zone Untrust screen ip-loose-src-route
set zone Untrust screen ip-strict-src-route
set zone Untrust screen ip-stream-opt

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

set zone Untrust screen icmp-fragment
set zone Untrust screen icmp-large
set zone Untrust screen syn-fin
set zone Untrust screen fin-no-ack
set zone Untrust screen limit-session
set zone Untrust screen syn-ack-ack-proxy
set zone Untrust screen block-frag

T. Configuring the Interfaces of the Netscreen Device

With the Netscreen 100, there are three physical interfaces. They are "Untrusted", "DMZ", and "Trusted". These interfaces are created during the initial setup. This is an example of what the GUI would look like. I assigned the corresponding IP to each interface as shown in the table below. I also assigned a 24-bit subnet mask for each network.

GUI
Network > Interfaces

Name	IP/Netmask	Zone	Type	Link
DMZ	192.168.25.1/24	DMZ	Layer3	up
trust	192.168.1.1/24	Trust	Layer3	up
untrust	xxx.xxx.xxx.xxx/24	Untrust	Layer3	up

CLI
set interface trust ip 192.168.1.1 255.255.255.0
set interface untrust ip xxx.xxx.xxx.xxx <netmask>
set interface dmz ip 192.168.24.1 255.255.255.0

U. Routing

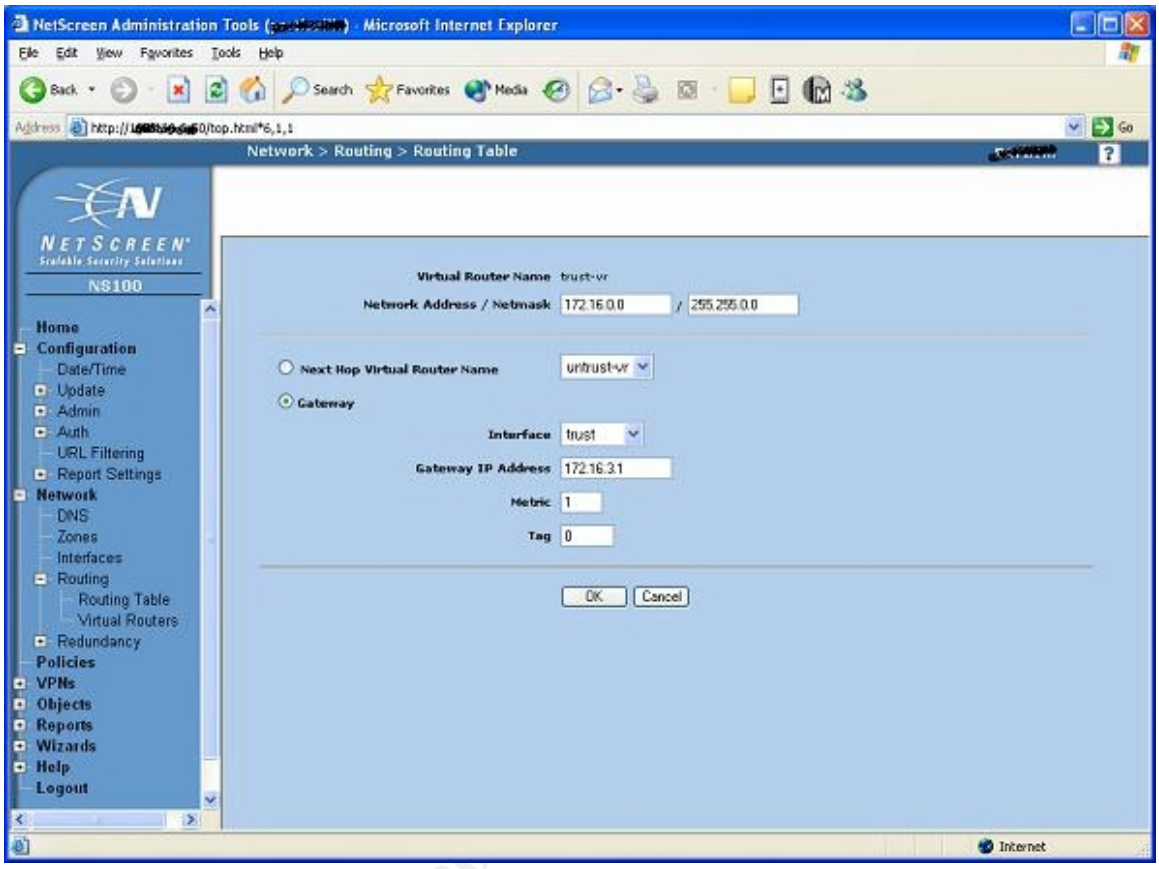
Netscreen, by default, creates the routes for your three interfaces. If you have multiple network segments, you may need to create additional routes to allow connectivity through your firewall like the example in the following table. Since our three network were added already by the interface configuration, I needed to add a static route for 172.16.0.0/16.

GUI
Network > Routing > Routing Table

If you have additional routes that need to be added select "Add" using the "trust-vr" option. Enter the Network Address and Netmask within the fields provided. Select "Gateway" and with the "Interface" option select the zone you are trying to add. More than likely it will be on the "Trusted" interface. Enter the "Gateway IP" field with that network's default gateway. In this example we are creating a default Class B network

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

using 172.16.0.0 as the Network and using a 24 bit netmask as 255.255.0.0. The default gateway would be 172.16.3.1. for our sample network.



CLI

set route 172.16.0.0/16 gateway 192.168.1.1 metric 20 tag 1

V. Policies

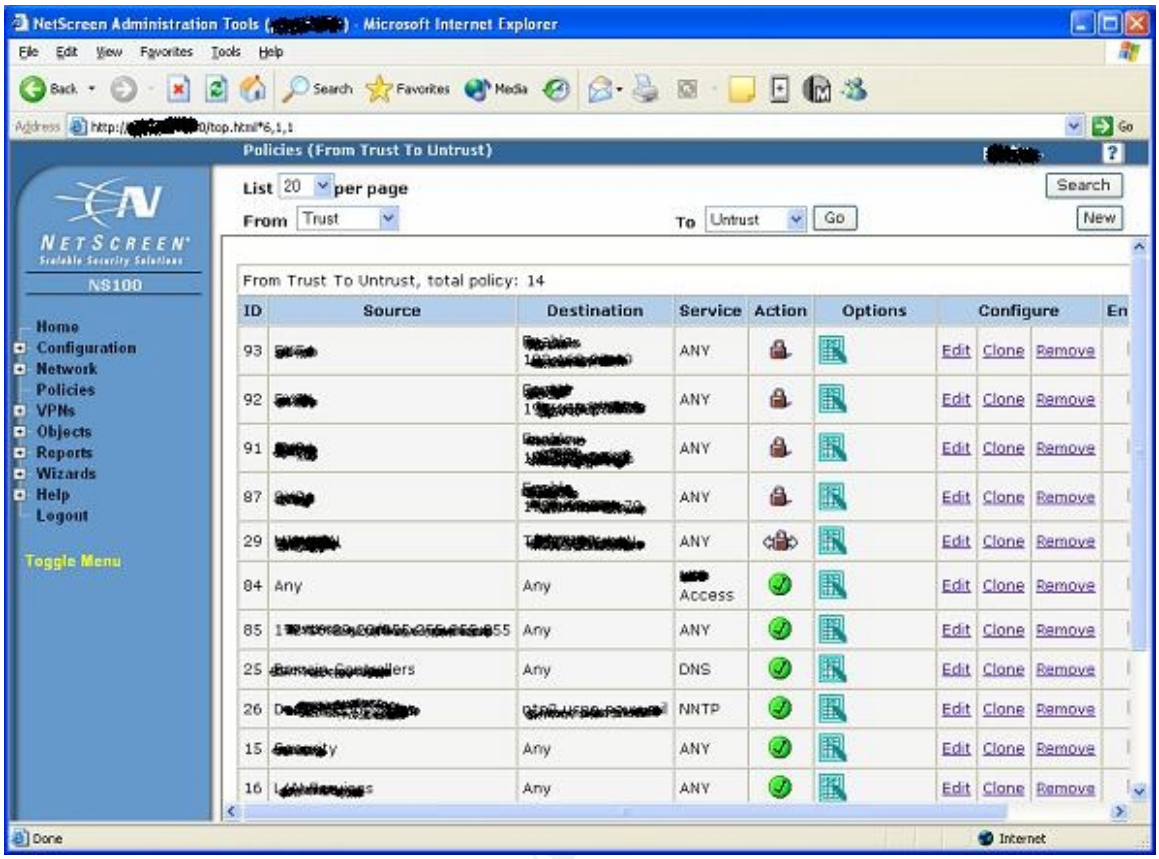
To create new policies using the GUI is relatively easy. Our organization no longer allowed services to be accessed by our external network to our internal network. All those devices were added to our DMZ. We no longer had incoming policies to our trusted network. We also restricted most of our network to only be able to use HTTP and HTTPS.

GUI

Policies >

To create new policies select "New" and choose the proper zone. For example if you need to create a new outgoing policy, you would select from "Trust" to "Untrust".

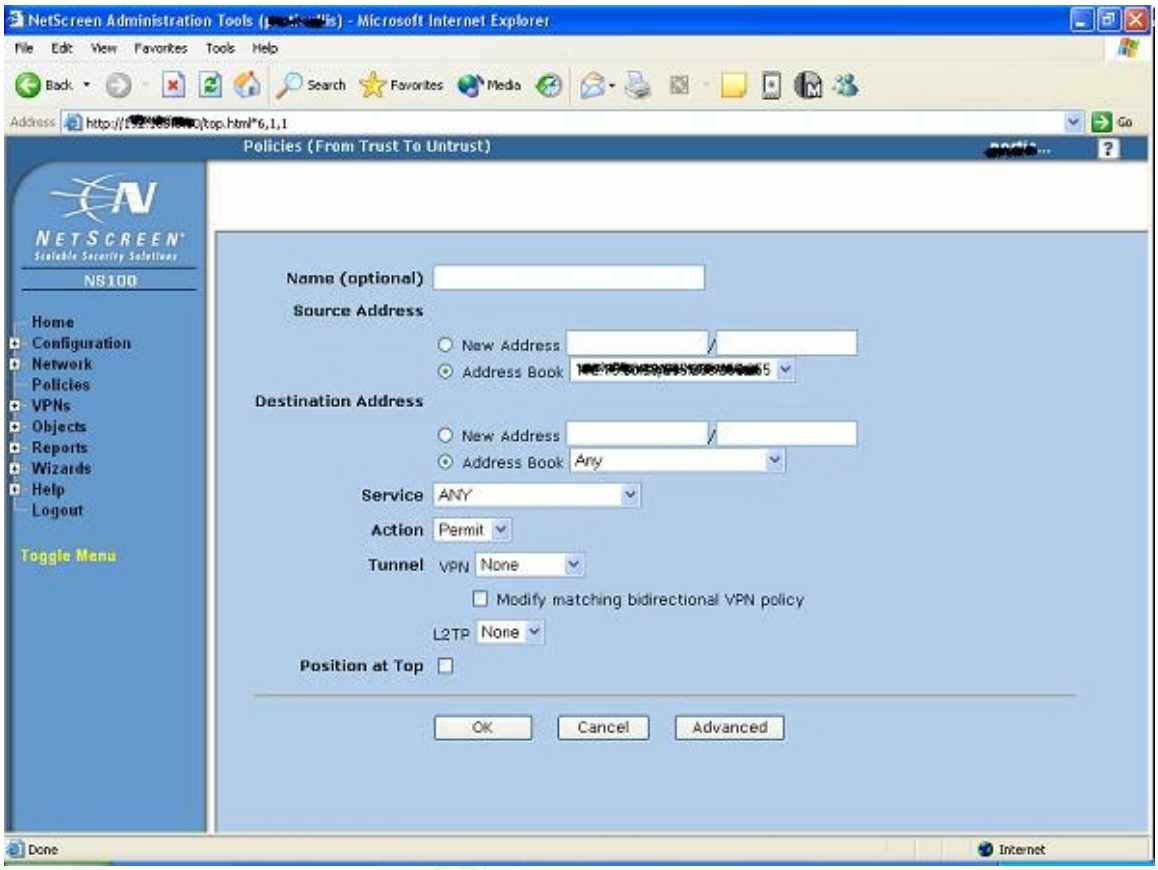
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



For security purposes, you would not want to create a policy from the untrusted network to the trusted network. You many want to create a Deny rule to log all activity for this rule for easy log review. To create a deny rule see the next section.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After you select the “New” button, the following screen will be shown.



Name Field: Optional
Source Address: Enter an address manually or choose one from your address book.
Destination Address: Enter an address manually or choose one from your address book**.**
Service: Choose of the many predefined services or one your customized services.
Action: To Permit, deny, or to tunnel (VPN)
Tunnel: If you chose to Tunnel as an action you would select which tunnel to use.
Position at Top: Can be selected if you want to place this particular policy at the top of all your policies for that direction..

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

CLI

Trust to Untrust

You may want only to allow specific services to be allowed outbound such as HTTP (port 80) and/or HTTPS (443) as a rule for the entire network.

set policy id 4 from "Trust" to "Untrust" "Any" "Any" "http" Permit log
set policy id 5 from "Trust" to "Untrust" "Any" "Any" "https" Permit log

Untrust to Trust

Ideally your organization will not allow inbound traffic from the untrusted side to your trusted network. A rule to deny everything and log all the "denies" may be beneficial in troubleshooting and anlysis.

set policy id 1 from "Untrust" to "Trust" "Any" "Any" "Any" Deny log

These are just a couple of simple policies. Your organization may have greater needs. If you do need to create additional policies, make sure you follow best practices by creating a simple rule at first with logging turned on so you can test and tweak the policy as necessary.

W. Services

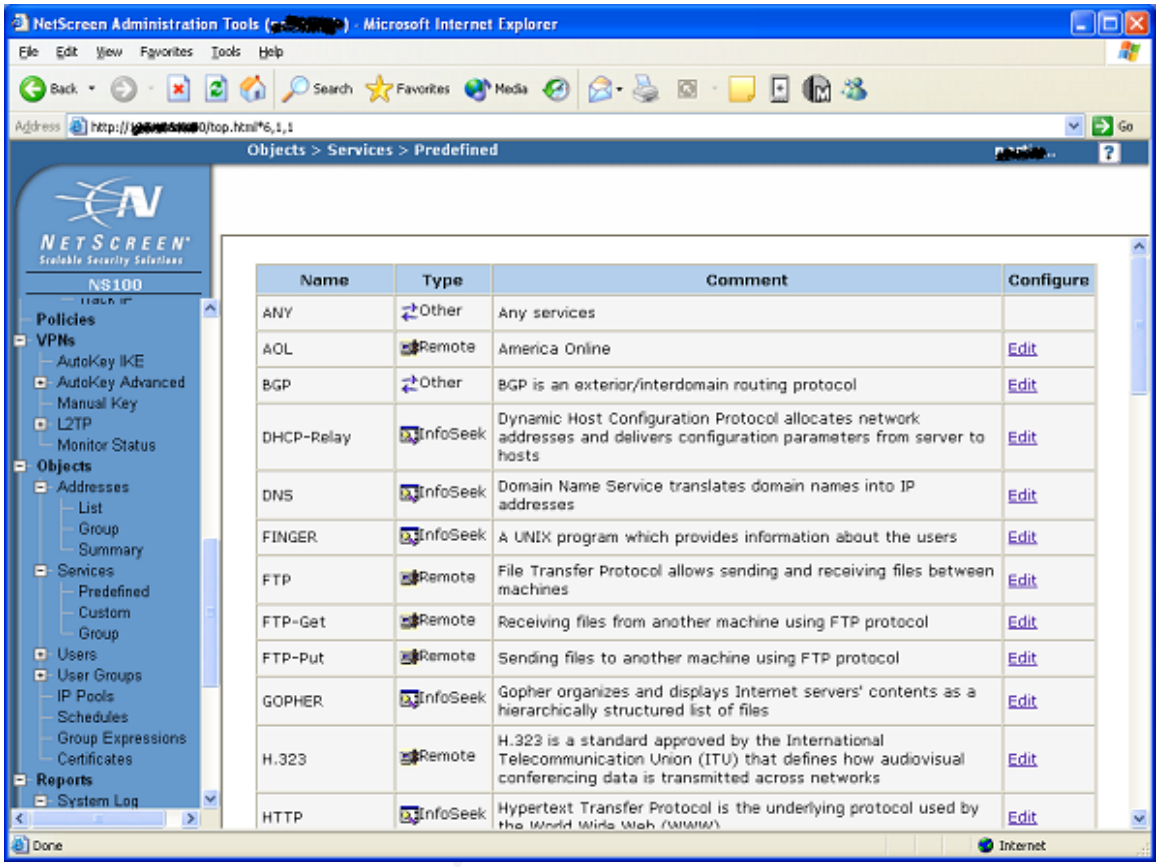
There are numerous services predefined by Netscreen. However you may need to use additional or uncommon services. This can be easily accomplished through creating your own custom services as shown in the next section. We had to create customized services to allow for use of Tripwire. Tripwire was being used to baseline our web servers and to monitor authorized and unauthorized changes to the servers.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GUI

Objects > Services > Predefined



CLI

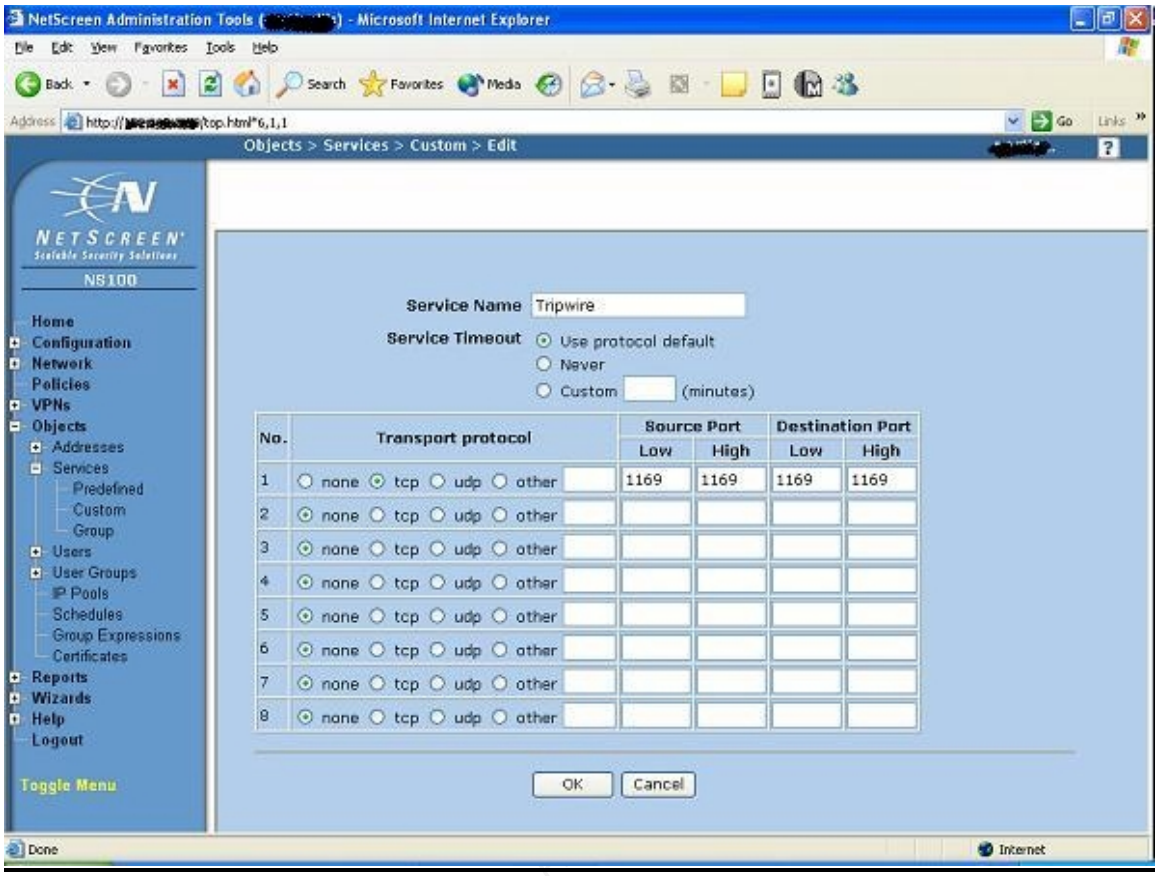
Since the predefined services are predetermined, there is no need to use the CLI unless just to see the predefined services. If you need to create customized services using the CLI, see the next topic.

get services pre-defined

Objects > Services > Custom

In this example, we are creating a new customized service for Tripwire. Since Tripwire uses TCP port 1169 we configure the necessary fields for use of this customized service. We installed Tripwire on our public web servers within our DMZ. This allowed us to monitor what changes were taking place and who was making them.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



CLI

set service Tripwire protocol 1169 src 1169-1169
set service Tripwire + tcp src 1169-1169 dst 1169-1169

© SANS Institute 2003,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IV. After

Upon completion of configuring and deploying our Netscreen 100 firewall, we had three zones. The first zone was our untrusted zone that communicated to our ISP. The second zone was our trusted network which communicated to our internal network. The last zone was our DMZ which had all our servers and devices that untrusted users needed to access. We off loaded our logs to a separate server which acted as our Syslog server. We now had only 7 routes compared to the 30 routes that had existed on our previous configuration.

Now, we also started to use NTP, logon banners, and email alerts when the firewall was encountering problems such as ICMP floods and WinNuke attacks. Procedures were developed on how to allow secure connections to our firewall for administration. The organization has also developed a better change control process to update the configuration and apply the patches.

V. Conclusion

Remember just because you have a firewall does not mean you are protected. You need to maintain and manage the firewall (or any other network security device!) regularly. This can be accomplished through daily administration tasks. Some of the procedures should include at a minimal

- Minimum Daily review of the Event, Self, and Policy logs (if not performing real time monitoring
- Update and patch the firewall as patches become available through defined change control procedures
- Perform backups as needed
- Intrusion Detection Procedures
- Incident Response Procedures

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References:

1) Zwicky, Elizabeth, Simon Cooper, and D Brent Chapman, Building Internet Firewalls, 2nd Edition, Sebastopol, O'Reilly & Associates, 2000
2) Northcutt, Stephen, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey, Network Perimeter Security, Indianapolis, New Riders, 2003
3) Garfinkel, Simon and Gene Spafford, Practical UNIX & Internet Security 2nd Edition, Sebastopol, O'Reilly & Associates, 1996
4) McClure, Stuart, Joel Scambray, and George Kurtz, Hacking Exposed – Network Security Secrets & Solutions 3Rd Edition, Berkeley, Osborne-McGrawHill, 2001
5) Millis, David, "Public NTP Time Servers", URL: http://www.eecis.udel.edu/~mills/ntp/servers.html
6) Curtis, John and Andy Hacker, The many uses of the word "switching", URL: URL: http://www.nwfusion.com/newsletters/lans/0413lan2.html
7) Netscreen, Company's Home Page URL: http://www.netscreen.com
8) Kiwi Syslog, Company's Home Page URL: http://www.kiwisyslog.com
9) WinSylog, Company's Home Page URL: http://www.winsyslog.com
10) WebTrends, Company's Home Page URL: http://www.netiq.com
11) Websense, Company's Home Page URL: http://www.websense.com
12) Netscreen Knowledgebase Article nskb606, **"**Upgrade Interrupted by Power Outage", URL: http://support.netscreen.com/eserverweb/esupport_customer/consumer/esupport.asp?id=nskb606

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.