

# *Securing/Configuring Windows NT Server*

**Authored By:** Jeffrey Fieldman

**Date:** May 27, 1999

**Purpose:** To help with the initial configuration as well as the hardening of Windows NT Server prior to the installation of Check Point's FireWall-1®

**Check Point Software Technologies LTD.**

---

**Preface:** This document will assist you in hardening/configuring Windows NT Server 4.0 prior to installing Check Point FireWall-1®. Consider this document a starting point; additional configurations may be required based on new service packs, patches, and hotfixes, as well as individual environment considerations.

### **BIOS Configuration:**

Set a password for entering the BIOS configuration and making changes. This will protect the system if someone has physical access to the firewall. Also, seal the computer case to reduce the chance of someone resetting the CMOS settings to remove the BIOS password protection.

In the BIOS boot-up configurations, disable the ability to boot from a floppy. Only the operating system drive should be set as the primary boot device; disable all other boot devices. However, we recommend leaving the ability to boot from the CD-ROM enabled until after you install Windows NT. If you do, disable CD-ROM booting after the Windows NT installation.

Also, disable any auxiliary ports that will not be used. These ports, which may be used to gain access to the system, include:

- parallel
- serial
- PS/2
- infrared
- USB

### **Initial Installation of Windows NT Server 4.0:**

We strongly recommended that you install the Windows NT operating system with the system disconnected from any network. This reduces the chances of contracting a virus, bacterium, worm, logic bomb, etc.

During the initial OS installation, you will be prompted for information that will help configure your Windows NT Server. Please note that the information you provide may be modified at a later time.

Make sure you choose the NTFS file system for the partition where the NT operating system and FireWall-1® software will reside. The NTFS file system's strict control of file resources helps prevent tampering of data, whether accidental or intentional.

The next portion of the configuration is the network interface setup. During this portion of the installation, you will be prompted to either select an interface from a list or allow

Windows NT Server to auto-detect one for you. We suggest that you allow Windows NT Server to auto-detect the network card for you. This will help to ensure you are using the appropriate drive. (Note: It is important to use the most current version of the network card's drivers.)

During this initial network card configuration, you will be prompted to select which protocols you want to bind to the interface card. **Select only TCP/IP** and deselect any other protocols that may be checked.

At the next prompt you will be asked if you would like to use DHCP to assign the IP address. **Select NO**. The installation program will then give you a screen for manually configuring of the IP address for the interfaces, DNS information, and other permanent configuration information.

If name resolution will not be available during the installation process, leave the DNS name server IP address entries blank. You may enter the DNS name server IP addresses after installing FireWall-1®.

Once you have completed the interface information, you will be prompted for identification information. You will first be asked for a **Computer Name** and whether it is part of a **Workgroup** or **Domain**. We recommend that you do not use names such as *firewall*, *fw1*, *myfirewall*, *myfw*, or *FW*, because using such names may allow hackers to realize the system is a firewall of some sort.

The next information you enter is only needed for Microsoft Networking (a service that will soon be disabled). Select **Workgroup** and give it a NON-reachable name (i.e., if you use Microsoft Networking, you should already have a workgroup name installed on your network. Simply choose a different name).

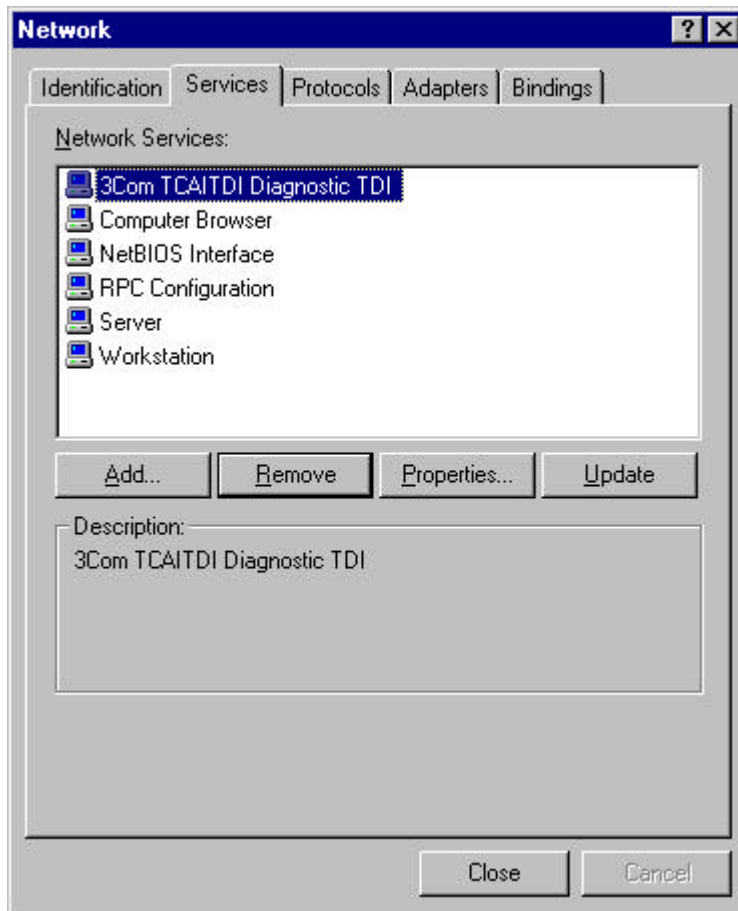
After you have entered the above-mentioned information, NT will complete the initial installation of the OS. Prior to making any additional OS modification, it is recommended that the most current Windows NT Service packs, hotfixes, and patches be installed. *Note: Please make sure the most current Windows NT Service pack, hotfixes, and patches are supported by Check Point. This information can be found at [www.checkpoint.com](http://www.checkpoint.com).*

### **Services:**

By default Windows NT Server installs the following services:

- **Computer Browser**
- **NetBIOS Interface**
- **RPC Configuration**
- **Server**
- **Workstation**

None of these services is needed for FireWall-1® to operate. To remove these services, click on **Start -> Settings -> Control Properties -> Networks**. From the **Network Menu**, click the **Services** tab. Once you have opened the Services tab you will see the above-mentioned services as well as any additional Services your installation has added. *Note: Additional services may be installed by your Network Card and may not be needed for proper operation of the machine. Please check with the manufacturer of your Network card to determine whether their service is needed for proper function of their card.*

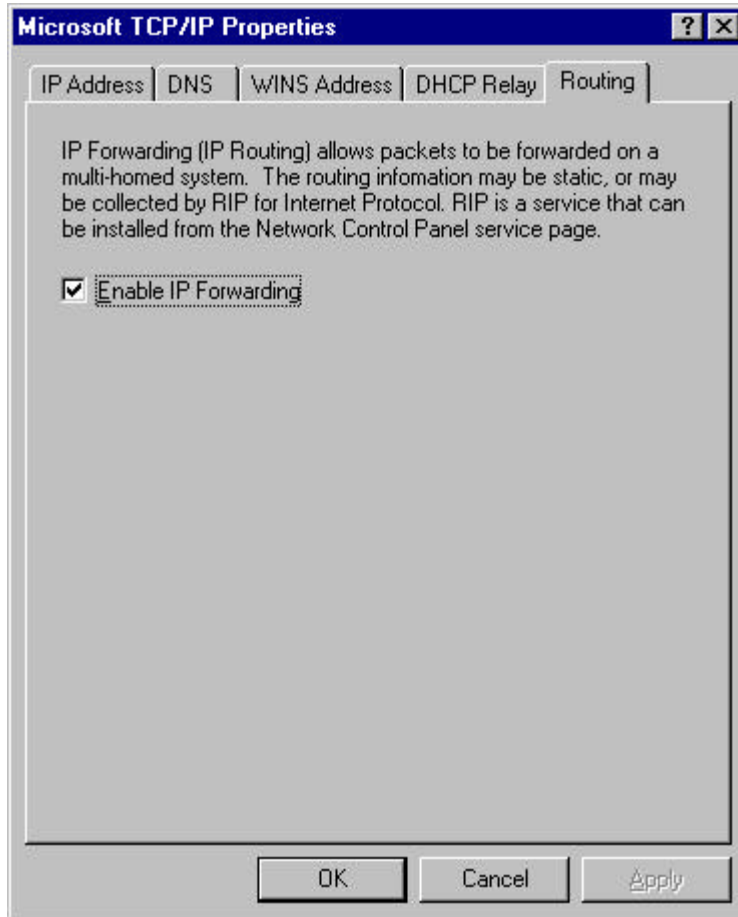


**IMPORTANT NOTE:** After you have removed the default services, it may be necessary for you to add one service. *If you are using a version of FireWall-1® prior to version 4.0 you need to add the SMNP service for the firewall to operate correctly.* If you are using FireWall-1® version 4.0, the SMNP service may be added for SMNP operations but is no longer required for proper FireWall-1® functionality.

At this time you may have to re-apply any Windows NT service packs, patches, and hotfixes you may have previously installed.

## IP Routing:

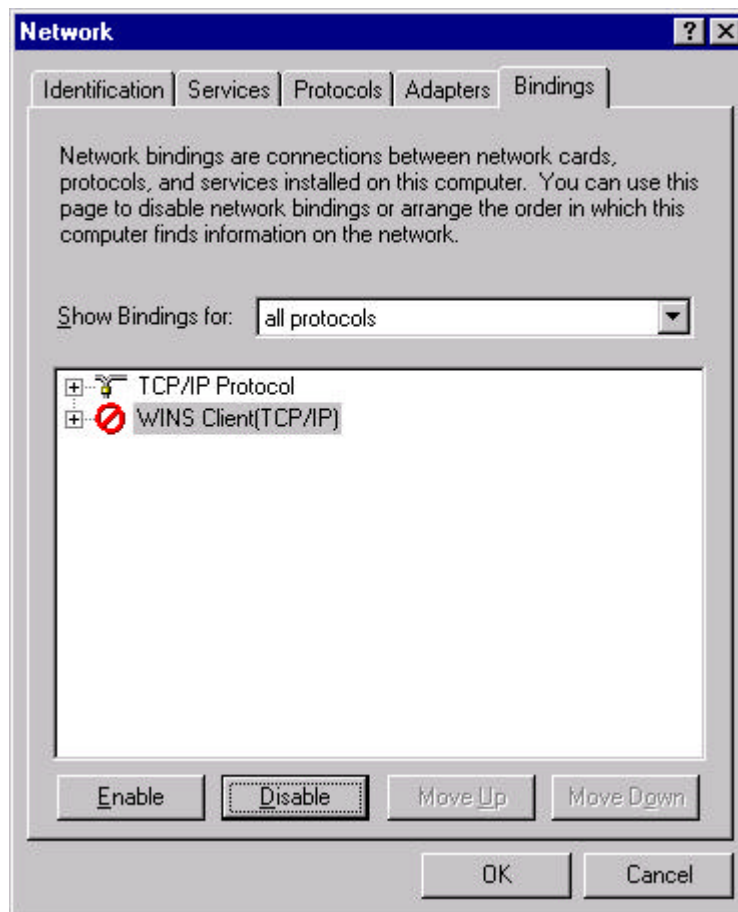
You must perform two IP routing configurations. The first is to make sure IP forwarding is enabled. To enable IP Forwarding, click on **Start -> Settings -> Control Properties -> Networks**. Click on the **Protocols** tab, then double click on **TCP/IP Protocol**. Click on the **Routing** tab and make sure the **Enable IP Forwarding** box is checked. Click **OK** when complete.



The second IP configuration confirms that you have defined a default route on your external interface. To ensure you have done this, click on **Start -> Settings -> Control Properties -> Networks**. Click on the **Protocol** tab. Next, double-click on the **TCP/IP Protocol**. Confirm that the **Default Gateway** has been set. *Note: None of your other interfaces should have a default gateway defined. If they do delete the entry.*

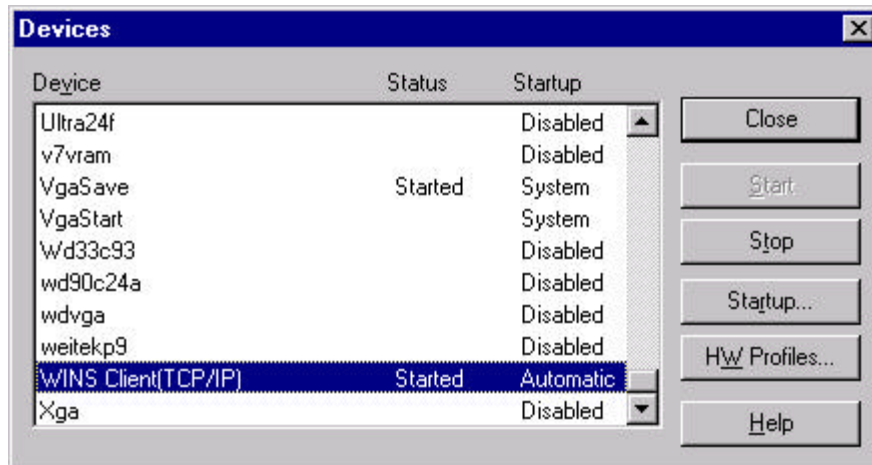
## WINS TCP/IP:

To disable **WINS TCP/IP**, click on the **Bindings** tab in the **Network** Menu. All services in the default listing will be displayed. If you followed the above steps correctly, there should not be any other services listed. Click on the pull-down menu labeled, “Show Bindings for:” and choose **all protocols**. In the **all protocols** menu, you will see **TCP/IP** and **WINS TCP/IP**. Select **WINS TCP/IP** and click the **Disable** button.



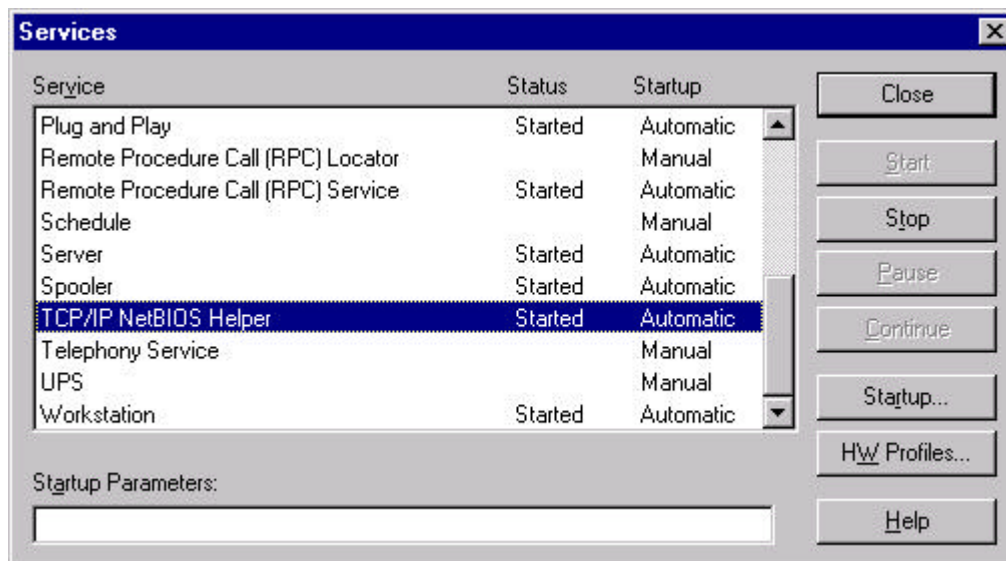
## Disabling other devices and services.

Now reboot your Windows NT Server and, after doing so, remove the WINS Client. To accomplish this click **Start -> Settings -> Control Properties -> Devices**.



Scroll down the device listing until you see **WINS Client(TCP/IP)**. The device is configured to start automatically during bootup. Highlight the **WINS Client(TCP/IP)** and click on the **Startup...** button. Select **Manual** and click on **OK**. Next, click the **Close** button to exit.

Now go to the **Services** menu in the **Control Properties** panel.



In the Services menu, select the **TCP/IP NetBIOS Helper** service. This is set to start automatically at bootup by default. Click the **Startup...** button, select **Manual**, and click on the **OK** button. Next, click the **Close** button to quit.

Once you have completed this step, reboot your Windows NT Server. You should not see any warning messages when the system has come back up. You have now removed all unnecessary network services that are installed by default.

## **Additional Recommendations for Securing the Windows NT Server:**

Listed below are some additional recommendations for securing Windows NT Server. A number of these changes include editing the registry. **If you are not familiar with editing the registry, you should not attempt to make these changes.** Even the smallest mistake can cause significant and far-reaching problems.

1. Rename the **ADMINISTRATOR** account.
2. Disable the **Guest** Account.
3. Make sure the C: drive is formatted NTFS.

### **Registry Changes:**

1. Disable display of last userid in the logon window

*Set DontDisplayLastUsername to 1*

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon (REG\_SZ)

2. Display warning message when logon to server

*Set LegalNoticeCaption to "Notice"*

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon (REG\_SZ)

3. Display warning message when logon to server

*Set LegalNoticeText to "Authorized users only"*

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon (REG\_SZ)

4. Control remote access to event logs

*Set RestrictGuestAccess to 1 on all event logs*

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\EventLog\[Log Name] (REG\_DWORD)

5. Disable listing of account names by anonymous users

*Set RestrictAnonymous to 1*

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSAName (REG\_DWORD)

6. Audit use of Scheduling service

***Set Submit Control to 1***

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSA\SubmitControl (REG\_DWORD)

7. Control ability to submit jobs to schedule service

***Restrict access to administrators on for the following registry key***

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Schedule

8. Disable listing of account names by anonymous users

***Set RestrictAnonymous to 1***

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSAName (REG\_DWORD)

9. Disable LanManager password Hash Support

***Set LMCompatibilityLevel to 2***

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\LSA (REG\_DWORD)

10. Disable caching of logon credentials

***Set CachedLogonsCount to 0***

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon (REG\_DWORD)

***NOTE: The above list only contains some of the more important registry changes. Additional changes may need to be made as new Windows NT Server service packs, hotfixes, and patches are released.***

**Additional Resources:**

Below are links to additional (documents) information on this subject.

1. <http://www.enteract.com/~lspitz/pubs.html>
2. <http://www.phoneboy.com/fw1/faq/0073.html>