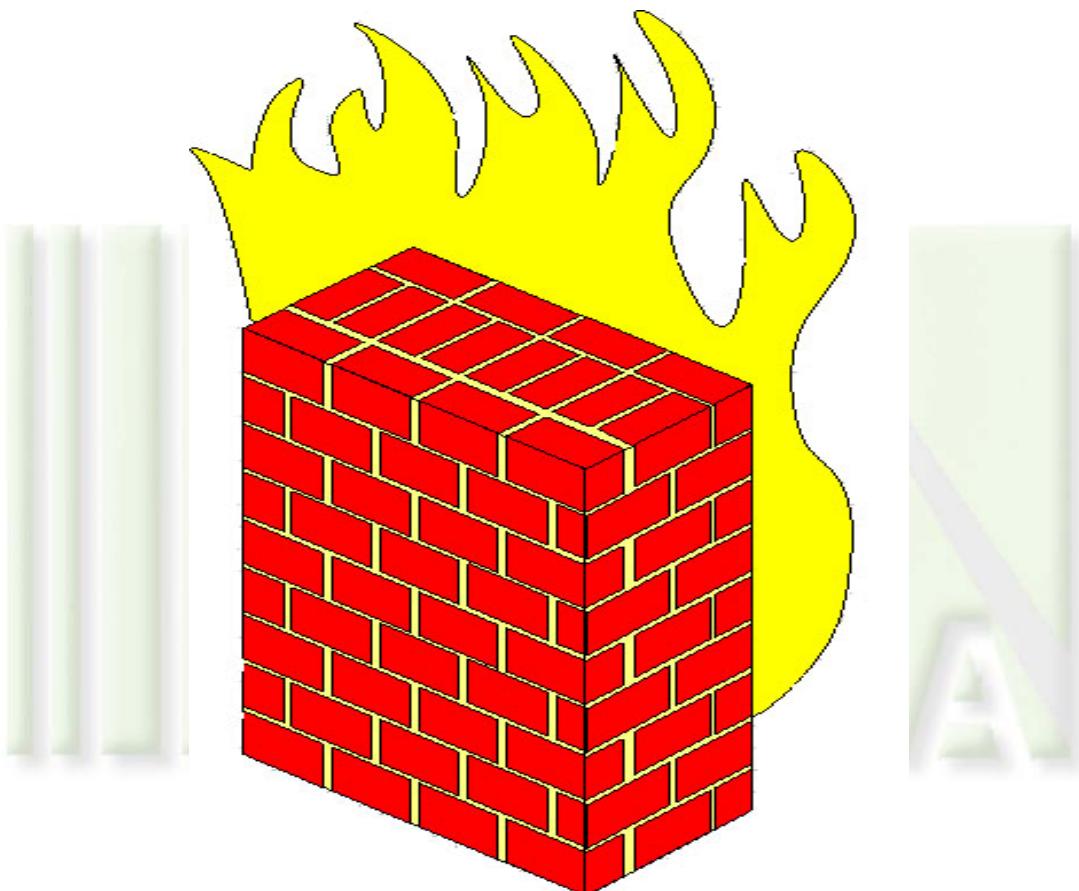


5.4.1

PERSONAL FIREWALLS

(Kerio)



March 2005



Laboratory Overview



Objective

At the end of this lab students will be able to configure and test a firewall.

Information for Laboratory

- A. Students will utilize Kerio Personal Firewall version 4 software

Student Preparation

The student will have completed requisite reading on firewalls. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

This lab will require that Internet explorer and CuteFTP be installed and working on each student computer.

Estimated Completion Time

60 Minutes

Firewalls

A firewall is simply a program or hardware device that filters data passing into or out of a network. Firewalls use different methods to control traffic flowing in and out of the network:

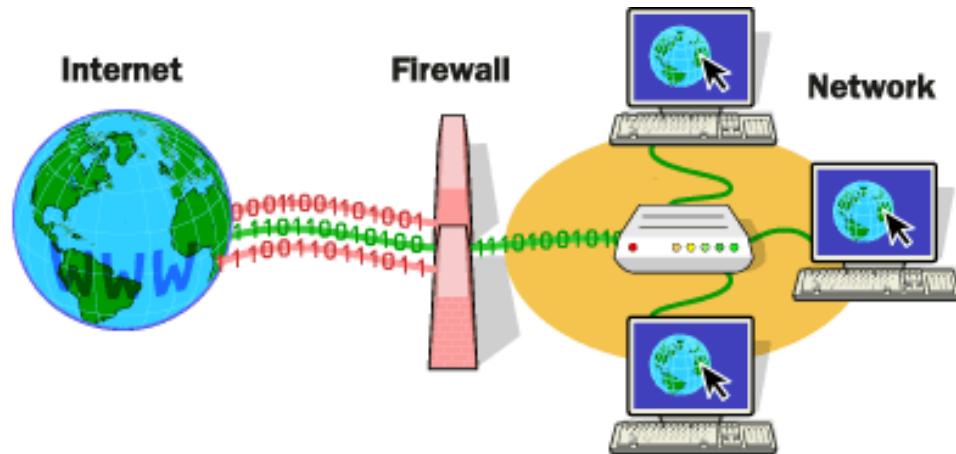
Packet filtering - Packets (small chunks of data) are analyzed against a set of filters, or rules. Packets that make it through the filters are sent to the requesting system and all others are discarded.

Stateful inspection - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information



traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

Most firewall configurations are setup to block access from outside or public networks, like the Internet.



Kerio Personal Firewall

Kerio Personal Firewall (KPF) helps users control how their computers exchange data with other computers on the Internet or local network. Kerio Personal Firewall prevents a single computer from attacks initiated by internal users. Remote workstations and laptops running Kerio Personal Firewall are protected from Internet born attacks. Kerio Personal Firewall has several functions, such as network security, privacy protection, intrusion detection, and application integrity.

Network security

Residing on each desktop computer, Kerio Personal Firewall allows advanced users or network administrators to create packet filter rules that block or limit traffic for specific ports, protocols, or IP addresses, adding a level of control and

security found in sophisticated network firewalls. Rules are based on the needs of individual users and the overall security requirements of an organization.

Scanning for sensitive information, blocking pop-up windows, filtering out on-line banner ads, and restricting cookies and spyware programs that track browsing habits are functions of KPF that reduce the risk of identity theft and help make surfing the Internet much more pleasant.

Intrusion detection

Potential intruders use various techniques to find out whether a targeted computer is vulnerable to attack. These techniques vary from simple port scanning to more elaborate exploits. Kerio Personal Firewall has a built-in intrusion detection system that identifies and blocks most known attacks.

Application integrity

Besides upgrades or updates, there is usually no need to modify an application. Some modifications can make your programs report usage information. Kerio Personal Firewall can keep applications from launching independently, being modified for malicious purposes, or starting other applications.

Step 1: Installing Kerio Personal Firewall

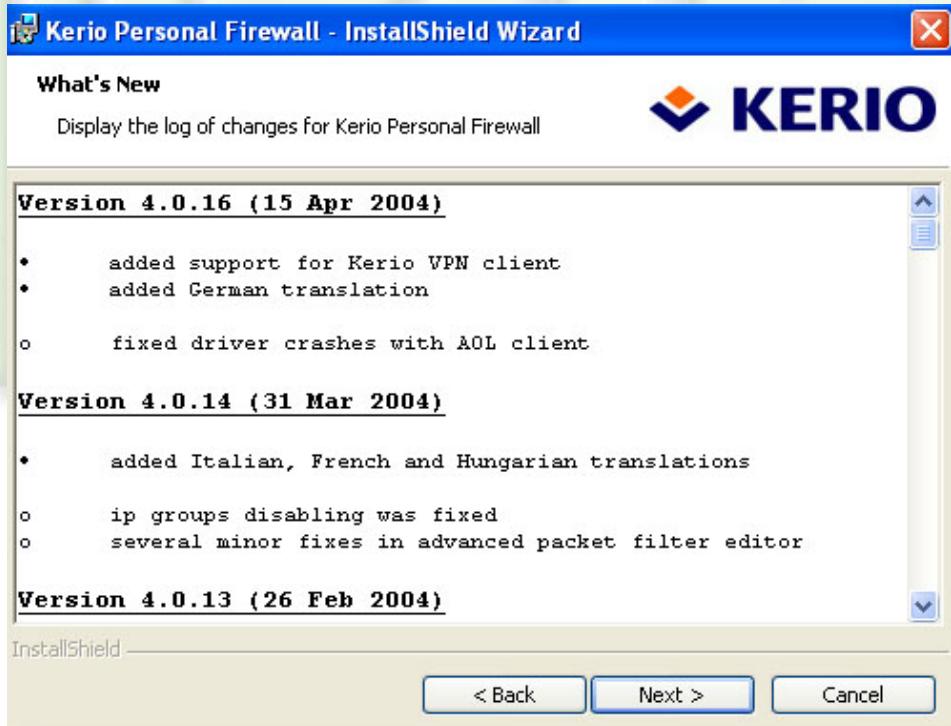
- (1) Locate the installation files for Kerio, and double click kerio-pf-4.0.16-en-win.exe to launch the setup program.



- (2) Click ok to choose English (United States)



(3) Click Next> to install



(4) Review the version change log and click Next>



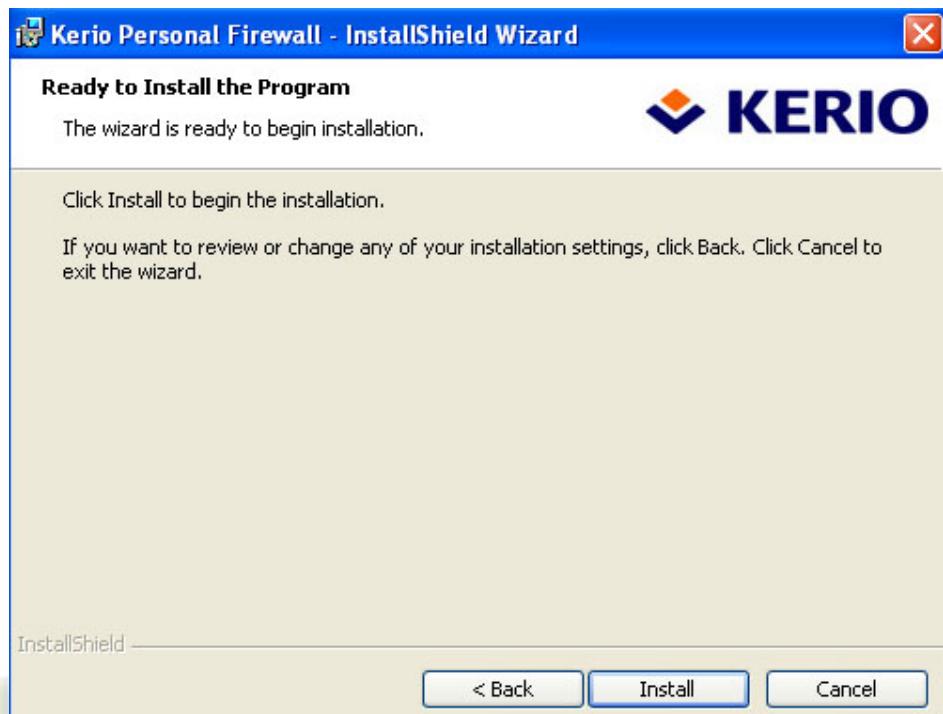


(5) Click the 'I accept the terms in the license agreement' radio button, and then click Next>



(6) Leave the destination folder to the default location C:\Program Files\Kerio\ and click Next>



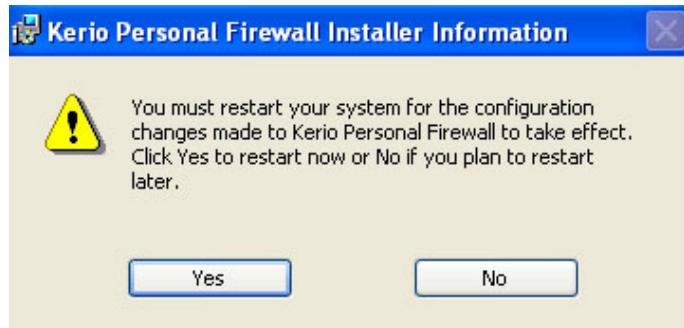


(7) Click Install to begin the installation



(8) After the Installation process, click Finish when prompted

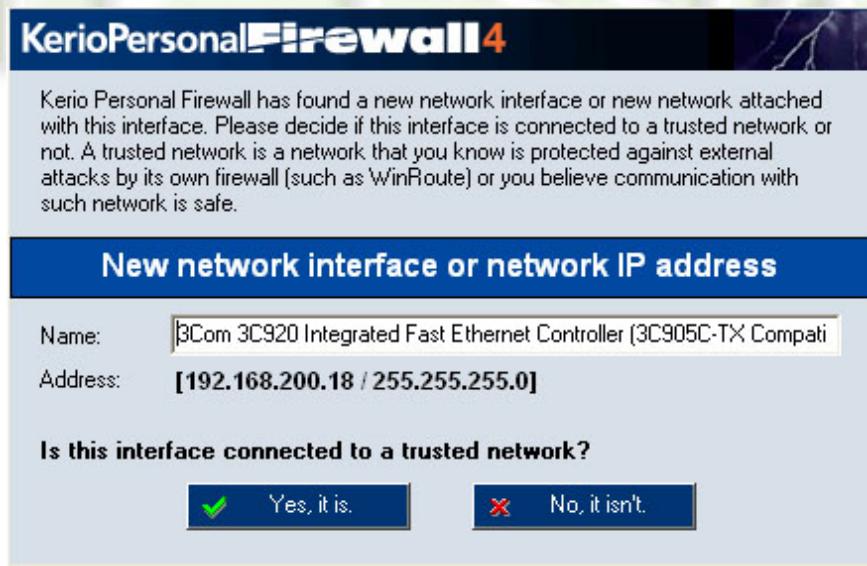




- (9) After the installation process is finished, you will be prompted to restart your computer for the configuration changes made to take effect. Click Yes to reboot.

Step 2: Configure Kerio Personal Firewall

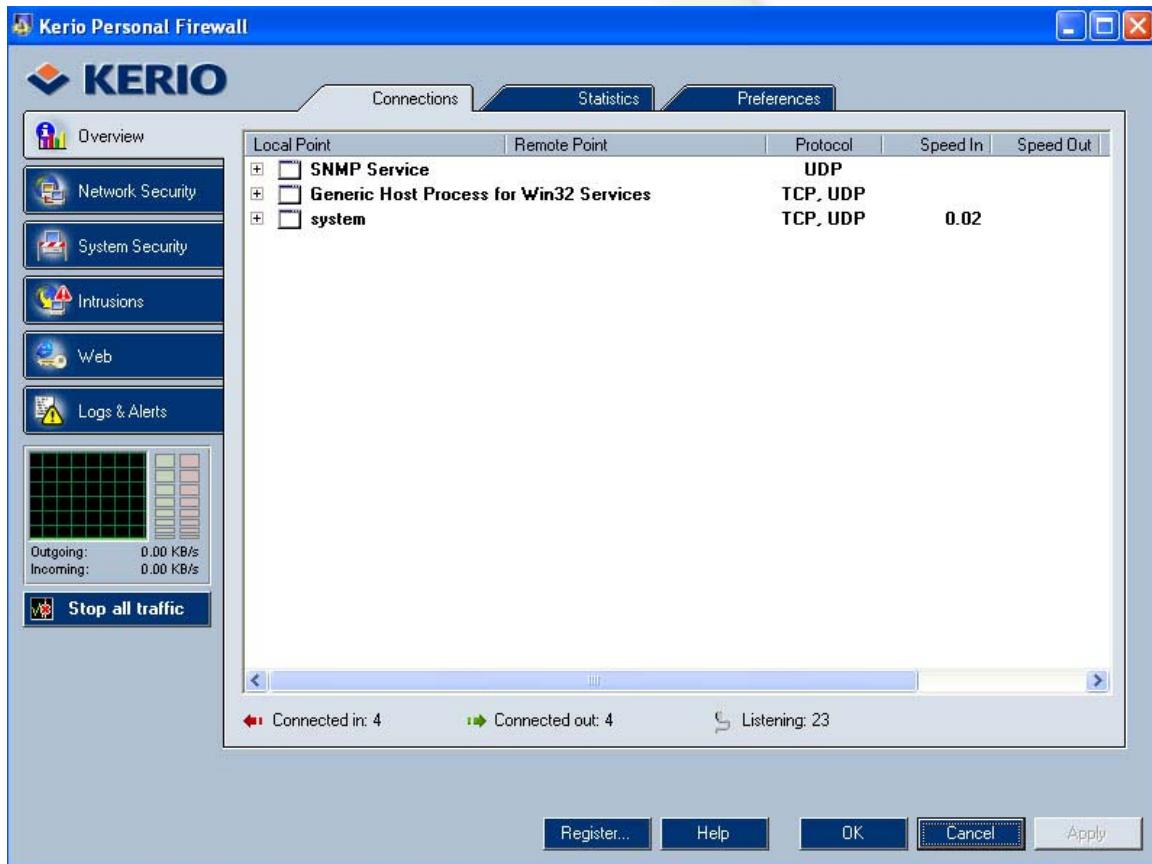
After the reboot, you will be prompted with a Kerio Personal Firewall New network interface or network IP address screen as below. This is part of the automatic basic configuration process of Kerio. This part of the setup identifies the private vs. public network addresses on your network. If you have more than one network interface installed in your computer, you will be prompted to choose if each interface is on a trusted network or not. A trusted network is a network that you know is protected against external attacks by its own firewall, or you believe communications with such network is safe. An untrusted network would be a direct connection to the Internet.



After choosing the appropriate setting for your network configuration (you may want to check with your instructor for the proper setting), you will notice that Kerio Personal Firewall is running in the background. The Blue shield icon next to the clock is for Kerio Personal Firewall.



Double click the Blue shield icon for KPF to launch the Kerio Personal Firewall user interface.

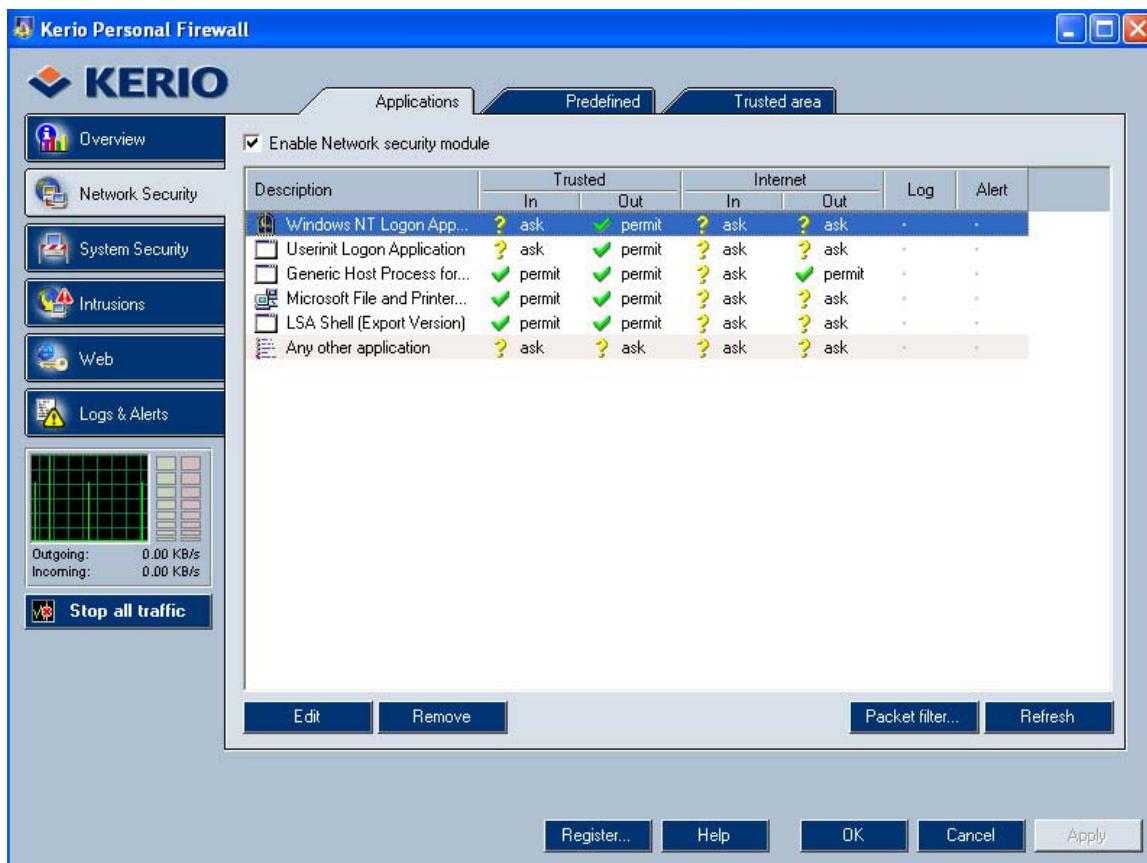


Within the interface, there are several informational pages, and several configurable option pages.

From the Overview page, Connections tab, to view the list of active connections and open ports used by individual

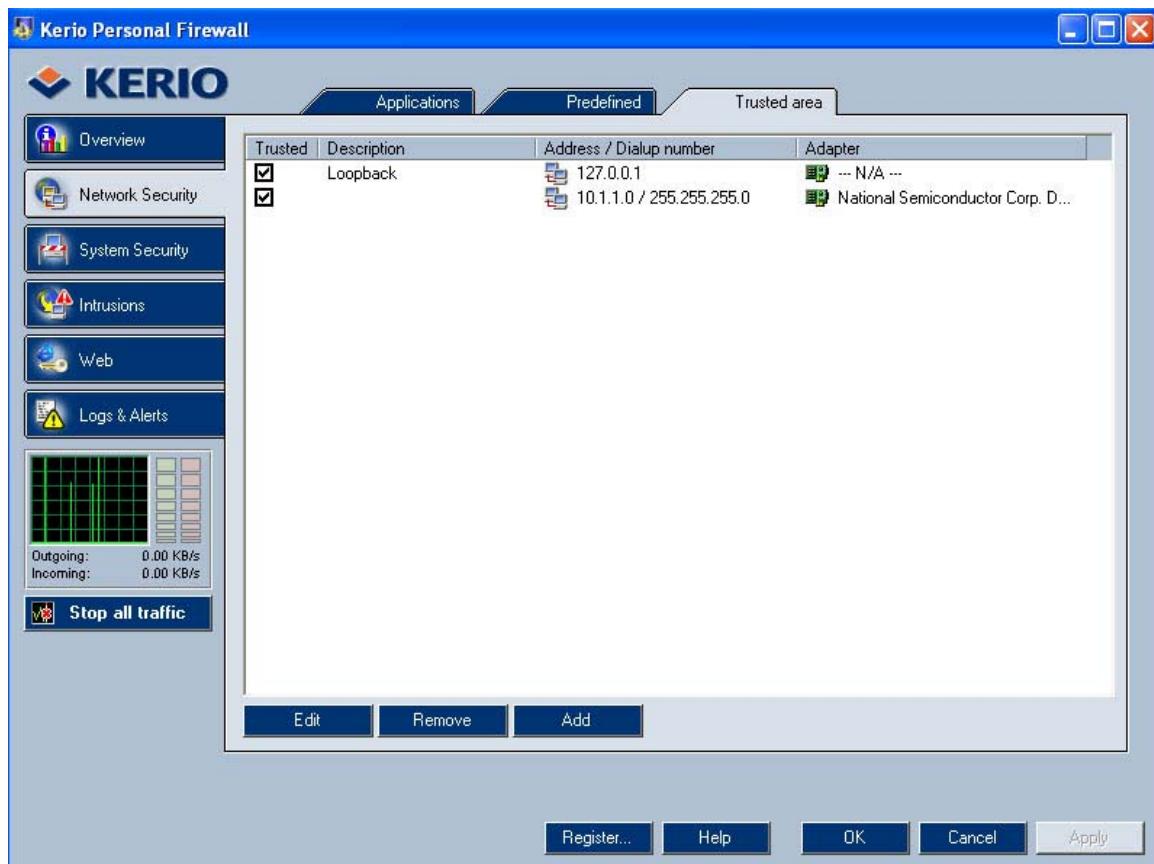


applications. This overview of connections makes users aware of which applications are actively involved in current network communication and which applications are waiting for connections.



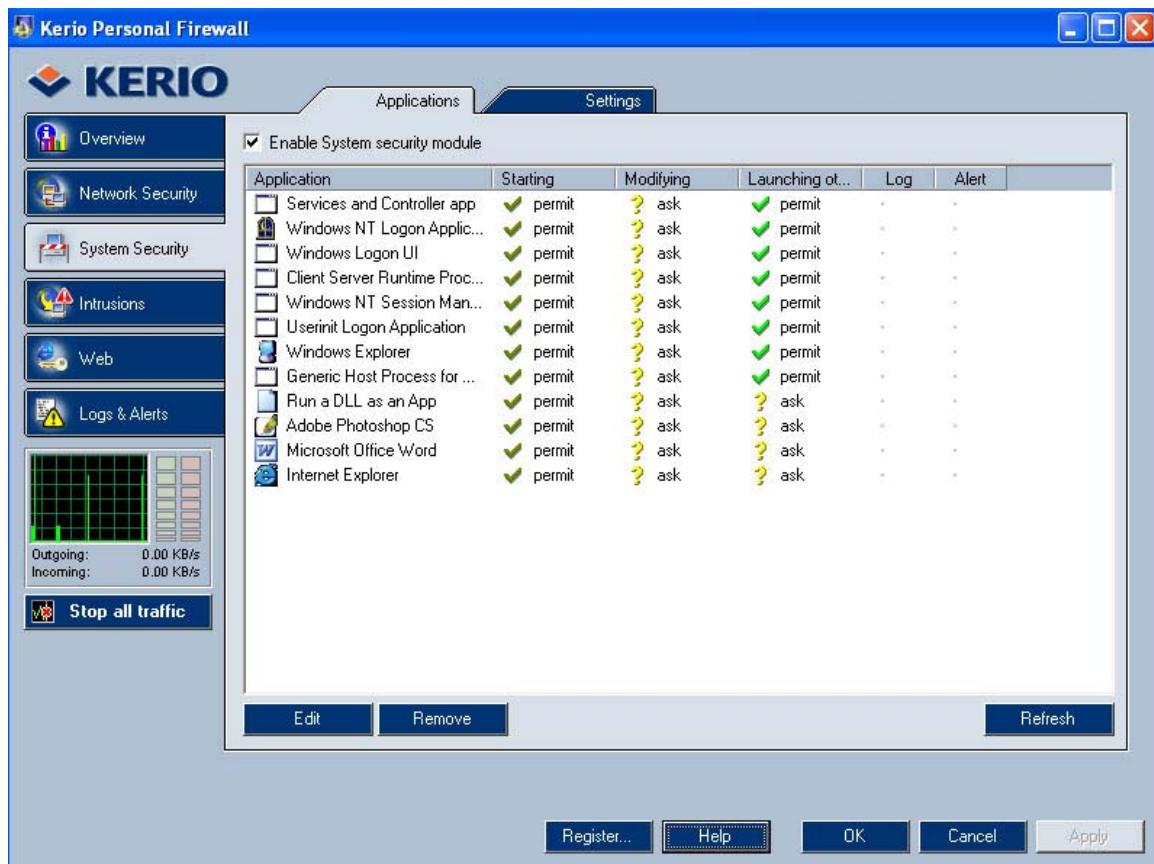
From the Network Security page, and Applications tab, you are able to configure which applications are allowed access to which network, either your trusted network, or the Internet. You may choose options to either Permit, Ask, or Deny access to an application to different parts of your network. Leave all the default settings the same for this lab.





From the Network Security page, Trusted area tab, you are able to edit the trusted networks on your network. When KPF first launched, it asked us to choose if our network interface card was connected to a trusted network. This is where that setting was automatically configured. Leave the current setting as is.





From the Applications tab in the System Security section, you can view and edit rules for startup and change of particular applications. These rules are based on interaction with user when an unknown application is started. Rules cannot be created by hand, they can only be edited or removed. When a unknown program is launched, a new rule is automatically generated, and the user is automatically asked what to do. Leave all current settings as is.



From the Intrusions section, you are able to choose security options for the KPF Intrusion Detection System (IDS). Click on the details button of each priority intrusion for a detailed explanation of all known intrusions, as below.

IDS details

Attack	Class
"BAD-TRAFFIC loopback traffic"	bad-unknown
"BAD-TRAFFIC same SRC/DST"	bad-unknown
"BAD-TRAFFIC Unassigned/Reserved IP"	non-standard-protocol
"BAD-TRAFFIC sys to multicast address"	bad-unknown
"DDOS TFn Probe"	attempted-recon
"DDOS Trin00\DaemontoMaster(PONGd...)	attempted-recon
"DDOS Trin00\DaemontoMaster(message...)"	attempted-dos
"DDOS Trin00\DaemontoMaster("HELL..."	attempted-dos
"DDOS Trin00\MasterDaemon(defaultp...)"	attempted-dos
"DDOS shaft handler to agent"	attempted-dos
"DDOS shaft agent to handler"	attempted-dos
"DDOS mstream agent to handler"	attempted-dos
"DDOS mstream handler to agent"	attempted-dos
"DDOS mstream handler ping to agent"	attempted-dos
"DDOS mstream agent pong to handler"	attempted-dos

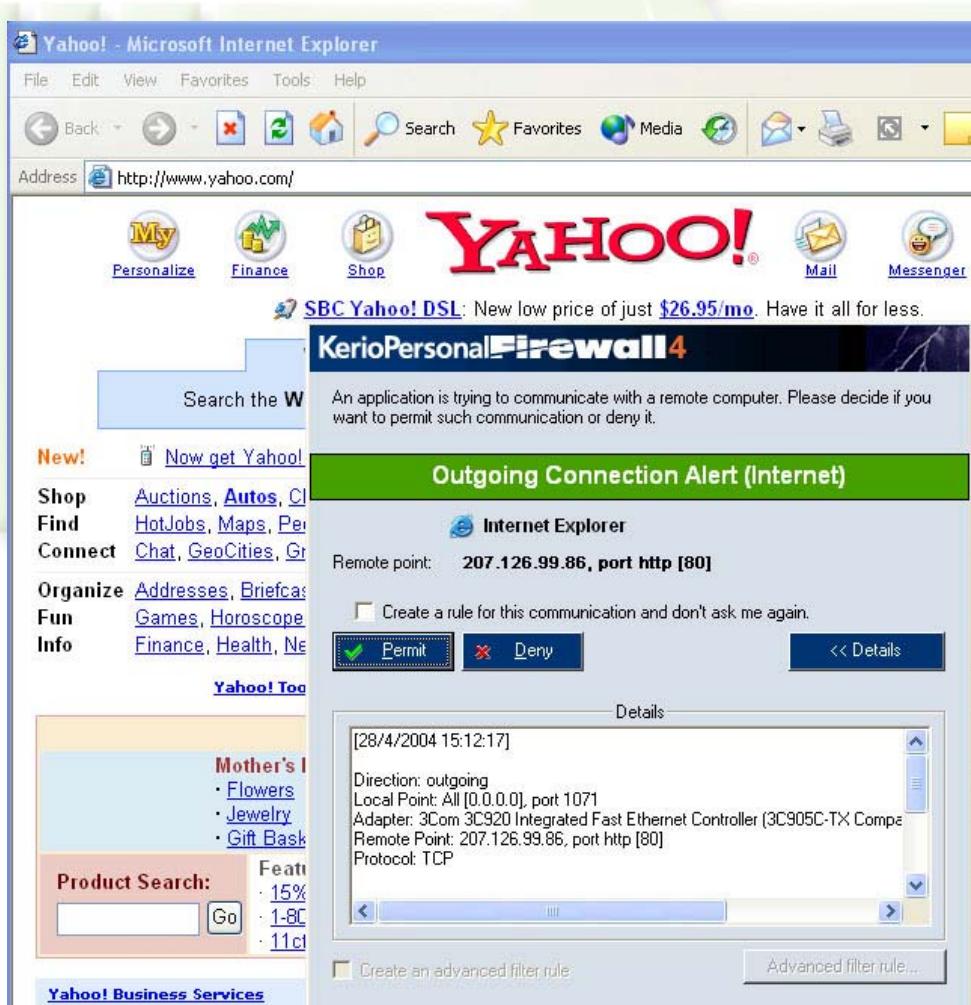


Step 3: Testing Kerio Personal Firewall

(1) Internet Explorer and HTTP traffic

Open Internet Explorer and enter www.yahoo.com in the Address bar. KPF should automatically prompt you with a Outgoing connection alert (Internet). There is information on the page describing what is happening, which application is used, traffic direction, Local Port in use, the used adapter (NIC), the remote IP address and port number, and the used protocol.

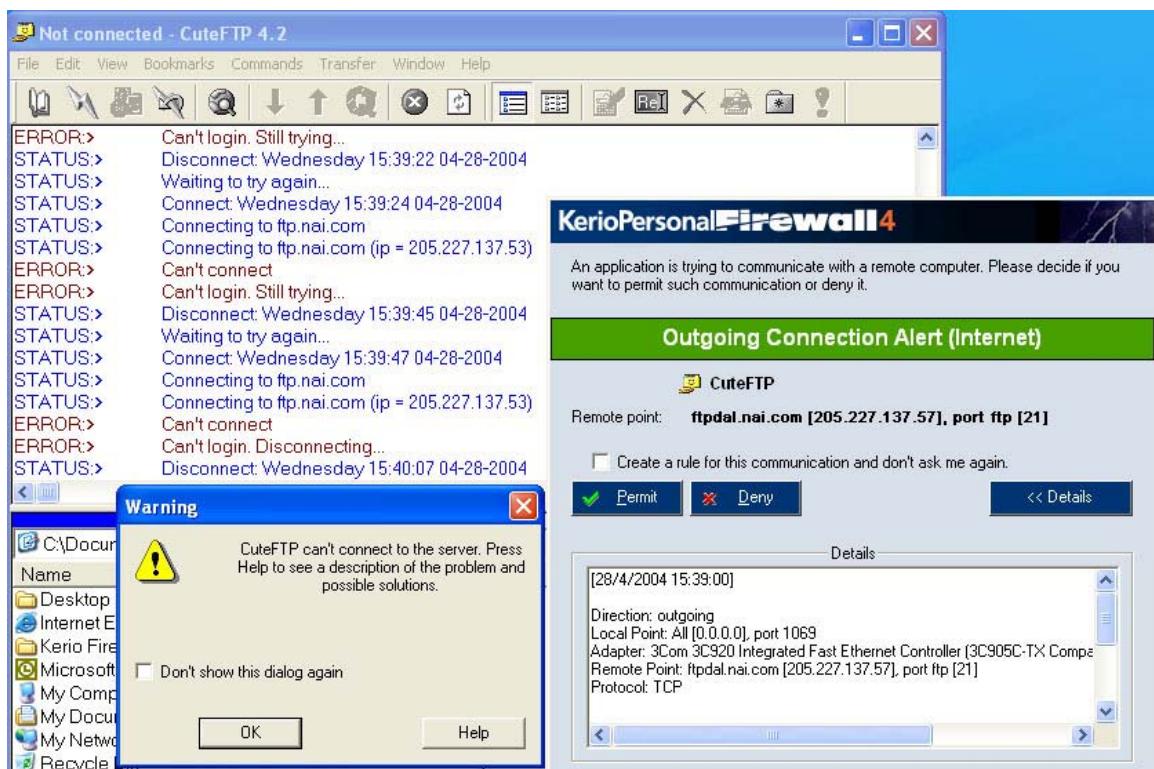
As the diagram below, you can see that the used application is Internet Explorer. The remote point is 207.126.99.86(may differ per user and session), TCP port 80 [http], on local port 1071 (may differ per user and session), and on the 3com 3c920 NIC.



From here you have to option to click deny access, or permit. Also, you can click the Create a rule for this communication and don't ask me again box. This will create a KPF rule, and automatically apply it for any future use. Click the Create rule box, and then click Permit. Yahoo's web page should then finish loading.

(2) CuteFTP and FTP Traffic

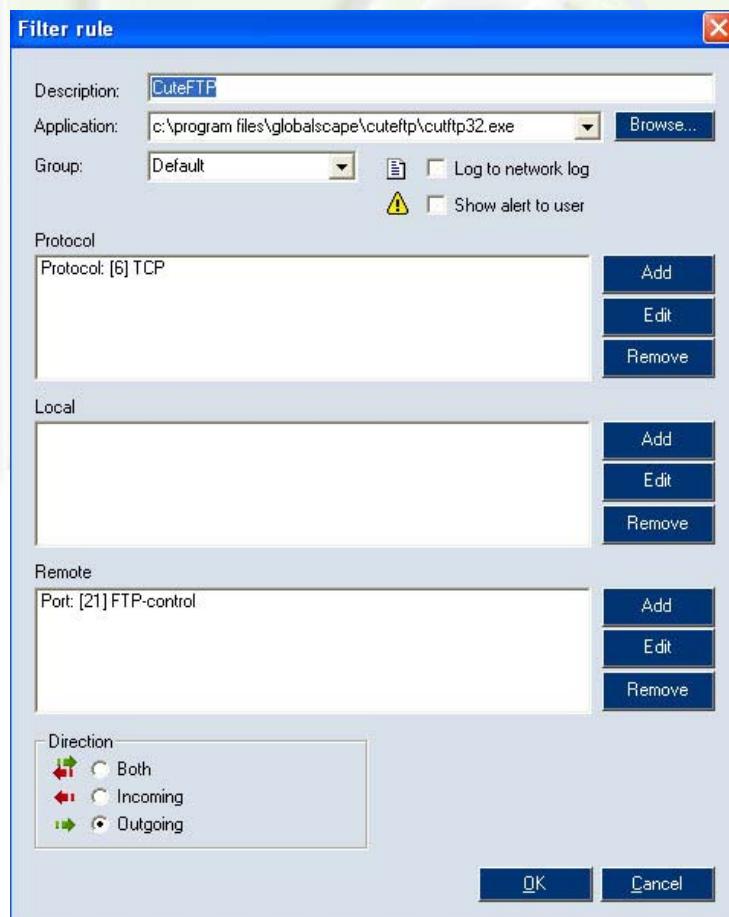
Open CuteFTP and attempt to connect to ftp.nai.com



KPF outgoing connection alert (Internet) will pop up as soon as you attempt to connect. Do nothing but watch CuteFtp as it attempts to connect. After a few attempts, CuteFtp will report that it can not connect to the server.

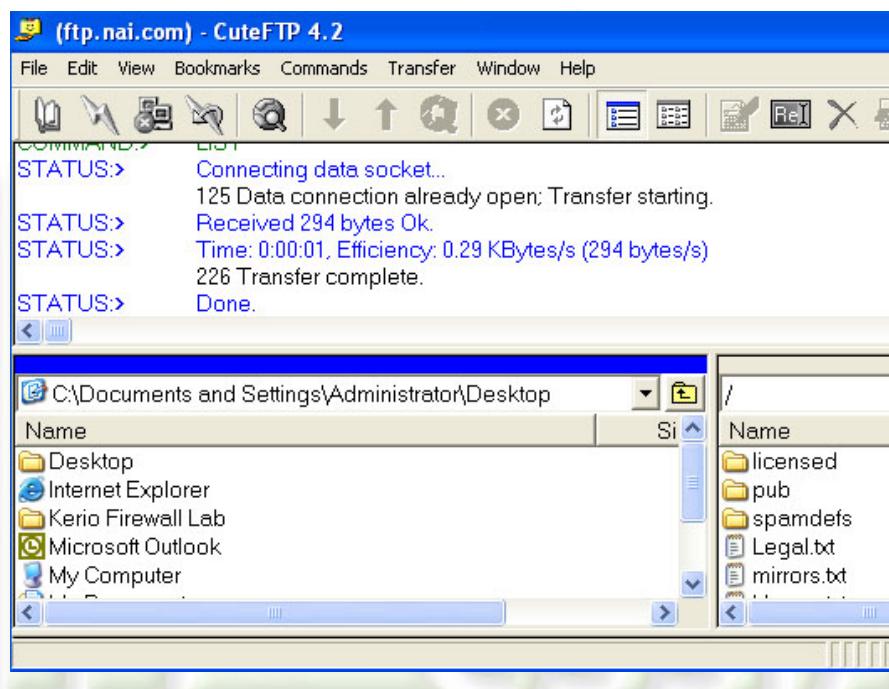
Now, from the KPF connection alert, click the Create a rule for this communication and don't ask again box, and click the Create an advanced rule filter, and then click Permit, as below.





Let KPF create the advanced filter rule, and click OK. To view the new Filter rule, go to the Network Security section, applications tab, and click on Packet filter on the bottom. You will see a listing of all filters. Double click on the CuteFtp rule, your output should look as above. Notice the settings, the application is listed with the executable file name and directory path, Protocol, Local and Remote ports, and the traffic direction. Click OK to save the new rule.

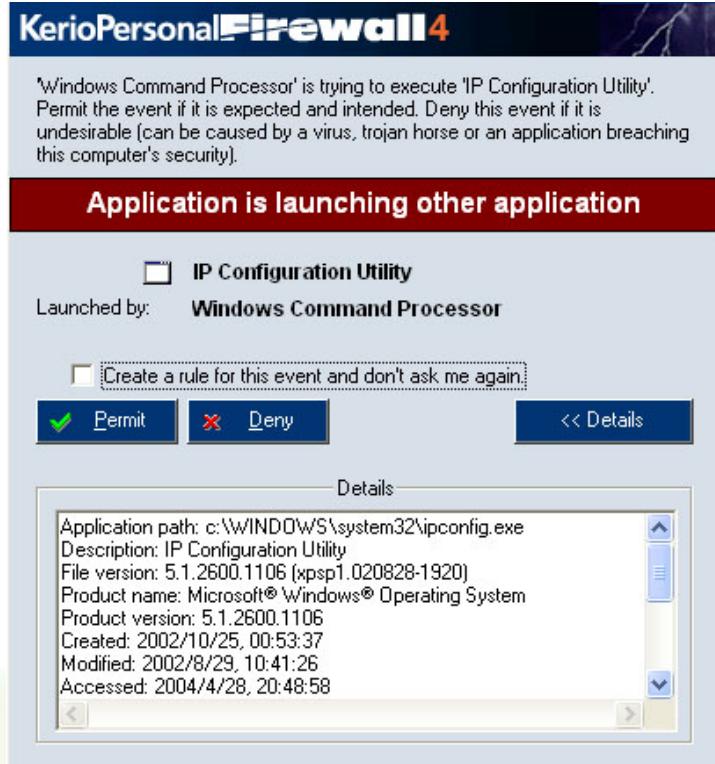
Now, with the saved rule, attempt to connect to ftp.nai.com once more. Your connection should be successful.



(3) IPCONFIG and PING

From START, Run, type 'cmd' and click OK. From the Command prompt, type 'ipconfig' and press enter.

KPF will prompt you with an Application is launching other application warning for IP Configuration Utility, launched by Windows Command Processor. Notice that the ipconfig command is not executed until you click permit.



```
C:\> C:\WINDOWS\system32\cmd.exe
C:\> Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . .
IP Address . . . . . : 192.168.200.18
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.200.1

C:\>
```

Notice your Default gateway address. Now from the command prompt, type 'ping ip address of your default gateway'
Example from above, 'ping 192.168.200.1'

KPF will prompt you with an Application is launching other application, TCP/IP Ping Command from Windows Command Processor.

Again, notice that the ping command is not executed until you click Permit. Click Permit, but DO NOT click the create a rule for this event, when you click permit.

```
C:\WINDOWS\system32\cmd.exe
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . .
IP Address . . . . . : 192.168.200.18
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.200.1

C:\>ping 192.168.200.1

Pinging 192.168.200.1 with 32 bytes of data:

Reply from 192.168.200.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.200.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Try the ping again, but this time click Deny. Notice that the ping command is terminated. Close all windows, and exit the Kerio Personal Firewall interface.

Step 4: Analysis

- 1) For which applications are firewalls best suited?
- 2) After working with Kerio Personal Firewall, what about single computer personal firewalls do you feel you should study further? Why?
- 3) Why should you setup a firewall on a computer that is connected to the Internet?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.



Appendix:

This lab was developed using Kerio v4.1.2, which can be obtained from:

<http://www.kerio.com>

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).

