_**IT Security** and Intellectual Property

Personal Firewalls

“Case study ::ZoneAlarm Security Suite”

Bashar Al Takrouri

Instructor:
Prof. Dr. Peter Rossbach

Summer 2006

EVERYTHING HE LOVES IS ABOUT TO BE USED AGAINST HIM.
FIREWALL
© 2006 WARNER BROS. ENTERTAINMENT

*source: http://movies.yahoo.com/movie/1808750745/info “February 10th, 2006 ”

What is firewall

Firewall is a piece of hardware and/or software which functions in a network environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.

The ultimate goal is: providing safe and controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model.

Usually, the internet (a zone with no trust) and an internal network (a zone with high trust).

Firewall techniques

Usually, multiple techniques are used to enhance the security level.

The main techniques are:

Packet filter: test each packet entering or leaving the network. It is typically done in a router.

Adv. Fairly effective and transparent to users.

Dis.
It is difficult to configure.
It is susceptible to IP spoofing .

Firewall techniques

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers.

Adv. It is very effective.

Dis. Can impose performance degradation.

Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established.

Proxy server: Intercepts all messages entering and leaving the network.
Adv. Hides the true network addresses. [1][2]

Firewall techniques

Stateful Inspection

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, and then incoming information is compared to these characteristics. [3]

Network Address Translation (NAT)

Allows one IP address, which is shown to the outside world, to refer to many IP addresses internally; one on each client station.[4]

Firewalls are customizable

Add or remove filters based on several conditions:

IP Address

Domain names

Protocols – allow and block different protocols such as:

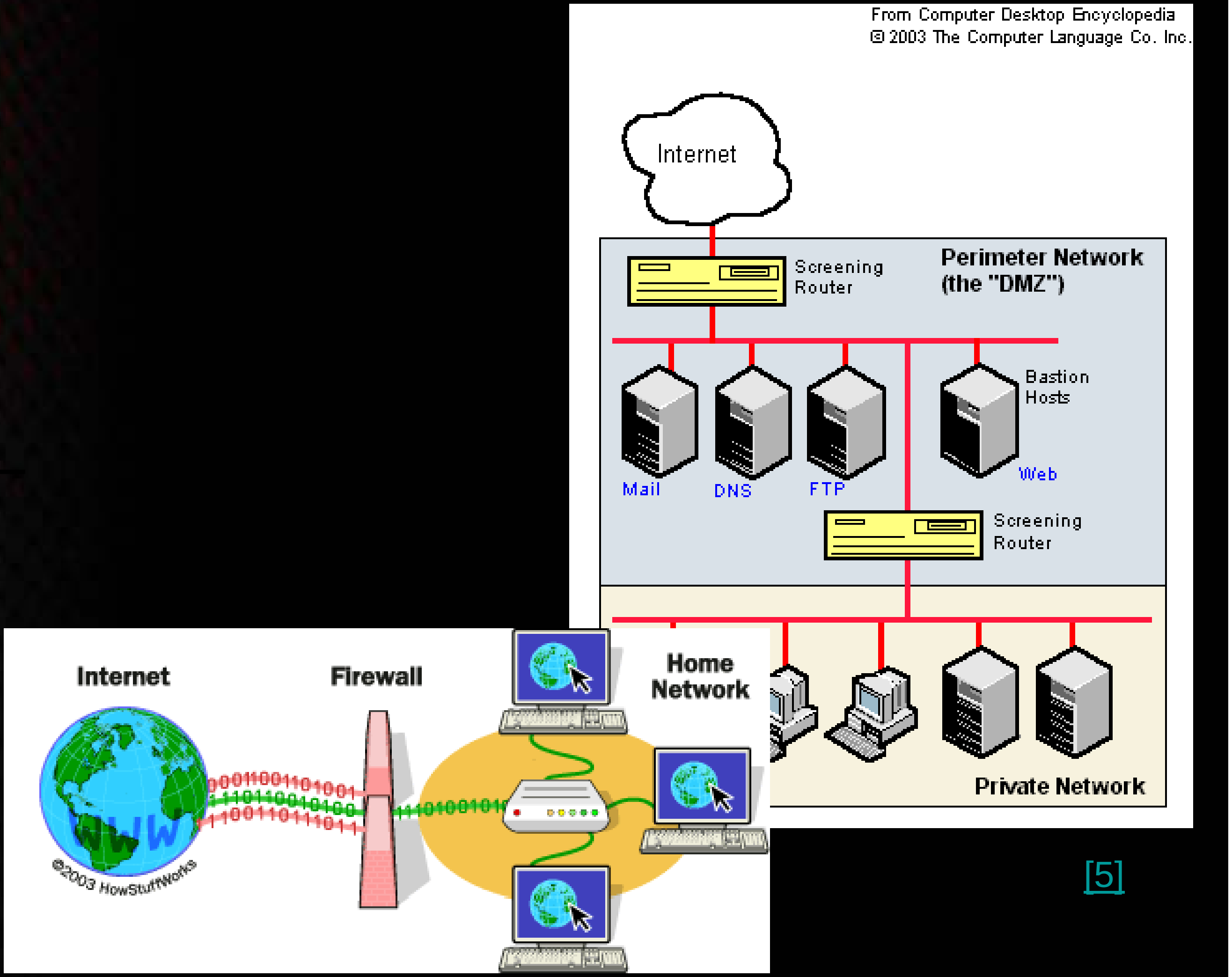
IP (internet protocol)

TCP (transmission control protocol)

HTTP (Hyper Text Transfer Protocol)

- **FTP** (File Transfer Protocol)
- **UDP** (User Datagram Protocol)
- **ICMP** (Internet Control Message Protocol)
- **SMTP** (Simple Mail Transport Protocol)
- **SNMP** (Simple Network Management Protocol)
- **Telnet**

Firewall techniques


From Computer Desktop Encyclopedia
© 2003 The Computer Language Co. Inc.

©2003 HowStuffWorks

[5]

Firewalls are customizable

Ports

Any server machine makes its services available to the Internet using numbered **ports**, one for each service that is available on the server.

For example, if a server machine is running a Web (HTTP) server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21. A company might block port 21 access on all machines but one inside the company. [6]

What does a basic PC firewall *not* do?

A PC firewall can't detect or remove computer viruses and worms if they're already on your computer.

Basic PC firewall can't clean up your computer after a virus attack; block phishing e-mails, spam, and pop-up ads; filter inappropriate or dangerous Web content; or shield IM users from spammers, thieves, and predators.

For complete protection beyond what a basic PC firewall provides, you need an integrated Internet security suite.[7]

Advanced protection PC firewalls

Dynamic firewalls

Dynamic PC firewall automatically opens your computer's door to the Internet when needed, allows only authorized traffic through, then immediately shuts the door.

Outbound and inbound protection

Many basic PC firewalls only protect your PC from unauthorized inbound communications. Some PC firewalls, protect your PC from unauthorized inbound as well as outbound communications. The transmission of your private data to the hacker would be an unauthorized outbound communication. [8]

Advanced protection PC firewalls

Remote login
Application backdoors
SMTP session hijacking
Operating system bugs
Denial of service
E-mail bombs
Macros
Viruses
Spam
Redirect bombs
Source routing

Case study

ZoneAlarm Security Suite

Advanced protection PC firewalls

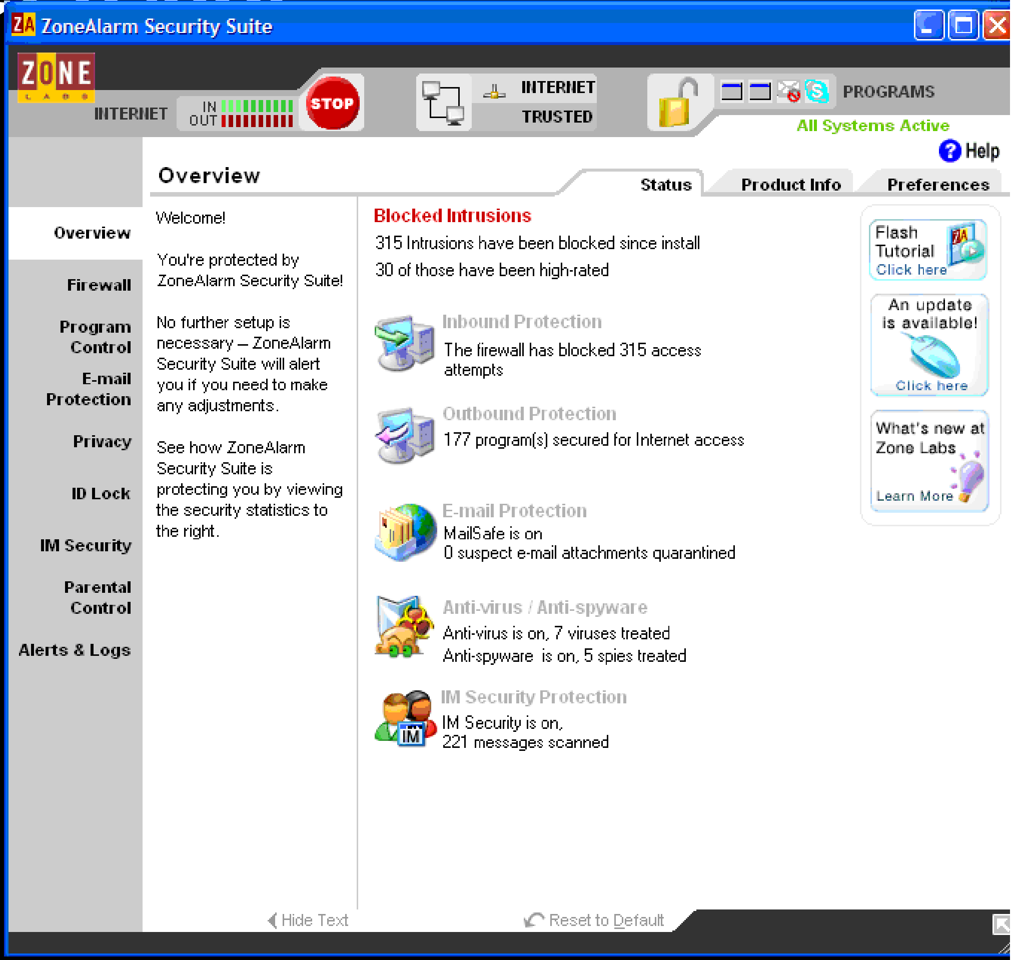
Basic configuration

Configuring program access permissions: Zone Labs security software can configure many of the most popular programs.

Joining the DefenseNet community

By joining DaefenseNet, you can help us focus our attention on the features and services that you use most often and to introduce new functionality that will provide even smarter security. The frequency of data transmission depends upon the configuration of your computer. For most users, data will be sent once per day.

Screenshot



Welcome!

You're protected by ZoneAlarm Security Suite!

No further setup is necessary – ZoneAlarm Security Suite will alert you if you need to make any adjustments.

See how ZoneAlarm Security Suite is protecting you by viewing the security statistics to the right.

Blocked Intrusions

315 Intrusions have been blocked since install

30 of those have been high-rated

Inbound Protection

The firewall has blocked 315 access attempts

Outbound Protection

177 program(s) secured for Internet access

E-mail Protection

MailSafe is on

0 suspect e-mail attachments quarantined

Anti-virus / Anti-spyware

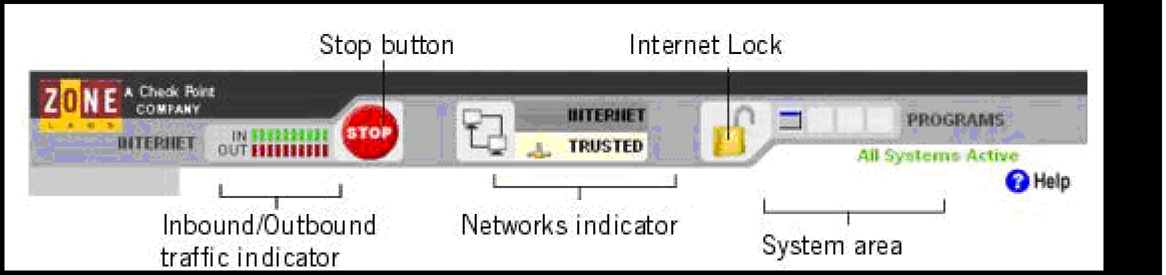
Anti-virus is on, 7 viruses treated

Anti-spyware is on, 5 spies treated

IM Security Protection

IM Security is on,

221 messages scanned



2006 © Bashar Al Takrouri| IT security| ISNM

Firewall configuration

Adjusting the security levels

High security setting: High security places your computer in *stealth mode*. Making it invisible to hackers. High security is the default configuration Internet Zone . (file and printer sharing is disabled; but outgoing DNS, outgoing DHCP, and broadcast/multicast are allowed, so that you are able to browse the Internet.)

Medium security setting: *component learning mode* based on the MD5 signatures. Medium security is the default setting for the Trusted Zone.

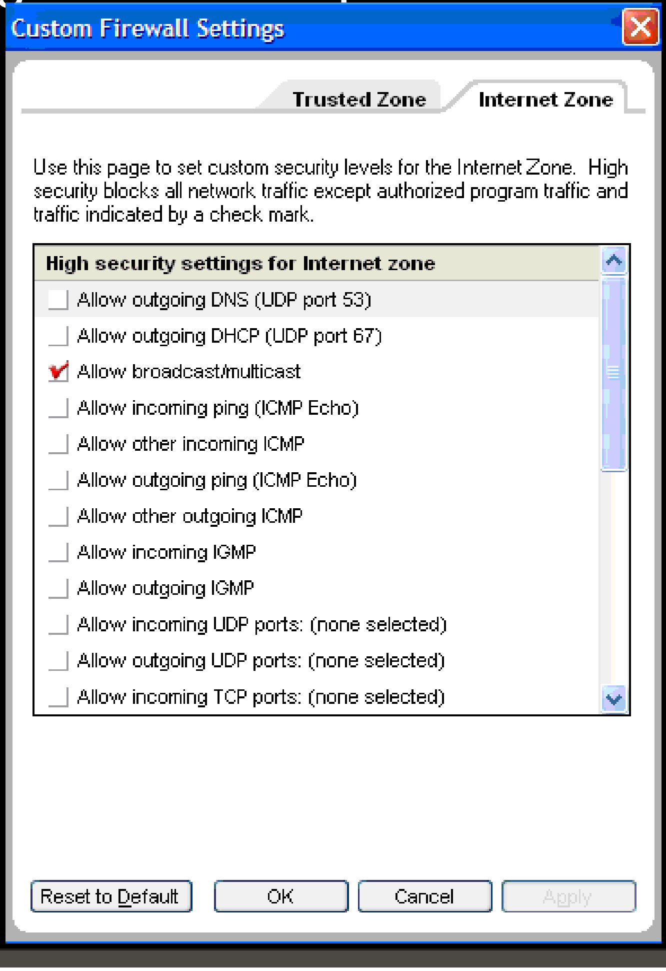
(File and printer sharing is enabled, and all ports and protocols are allowed. Icoming NetBIOS traffic is blocked. This protects your computer from possible attacks no stealth mode.)

Setting general security options

Block all fragments	Blocks all incomplete (fragmented) IP data packets. Hackers sometimes create fragmented packets to bypass or disrupt network devices that read packet headers.
Block trusted servers	Prevents all programs on your computer from acting as servers to the Trusted Zone. Note that this setting overrides permissions granted in the Programs panel.
Block Internet servers	Prevents all programs on your computer from acting as servers to the Internet Zone. Note that this setting overrides permissions granted in the Programs panel.
Enable ARP protection	Blocks all incoming ARP (Address Resolution Protocol) requests except broadcast requests for the address of the target computer. Also blocks all incoming ARP replies except those in response to outgoing ARP requests.
Allow VPN Protocols	Allows the use of VPN protocols (ESP, AH, GRE, SKIP) even when High security is applied. With this option disabled, these protocols are allowed only at Medium security.
Allow uncommon protocols at high security	Allows the use of protocols other than ESP, AH, GRE, and SKIP, at High security.
Lock hosts file	Prevents your computer's hosts file from being modified by hackers through sprayer or Trojan horses. Because some legitimate programs need to modify your hosts file in order to function, this option is turned off by default.

Adding custom ports

You can allow communication through additional ports at High security, or block additional ports at Medium security by specifying individual port numbers or port ranges.



Use this page to set custom security levels for the Internet Zone. High security blocks all network traffic except authorized program traffic and traffic indicated by a check mark.

High security settings for Internet zone

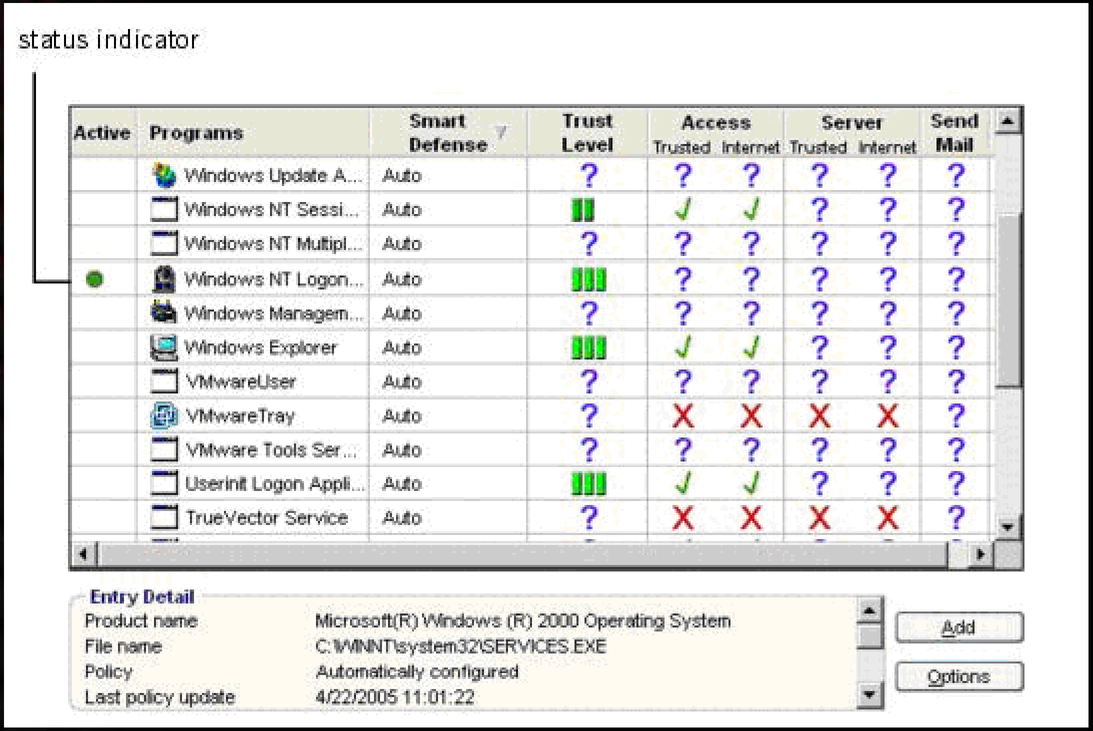
- ☐ Allow outgoing DNS (UDP port 53)
- ☐ Allow outgoing DHCP (UDP port 67)
- ☑ Allow broadcast/multicast
- ☐ Allow incoming ping (ICMP Echo)
- ☐ Allow other incoming ICMP
- ☐ Allow outgoing ping (ICMP Echo)
- ☐ Allow other outgoing ICMP
- ☐ Allow incoming IGMP
- ☐ Allow outgoing IGMP
- ☐ Allow incoming UDP ports: (none selected)
- ☐ Allow outgoing UDP ports: (none selected)
- ☐ Allow incoming TCP ports: (none selected)

Using the programs list

The programs list provides an overview of the programs on your computer that have tried to access the Internet or the local network.

The SmartDefense Advisor and Trust Level columns indicate OSFirewall Protection for your computer and specify whether a program is allowed to perform operating system-level actions like changing TCP/IP parameters, loading or installing drivers, or changing your browser's default settings.

Using the programs list



status indicator

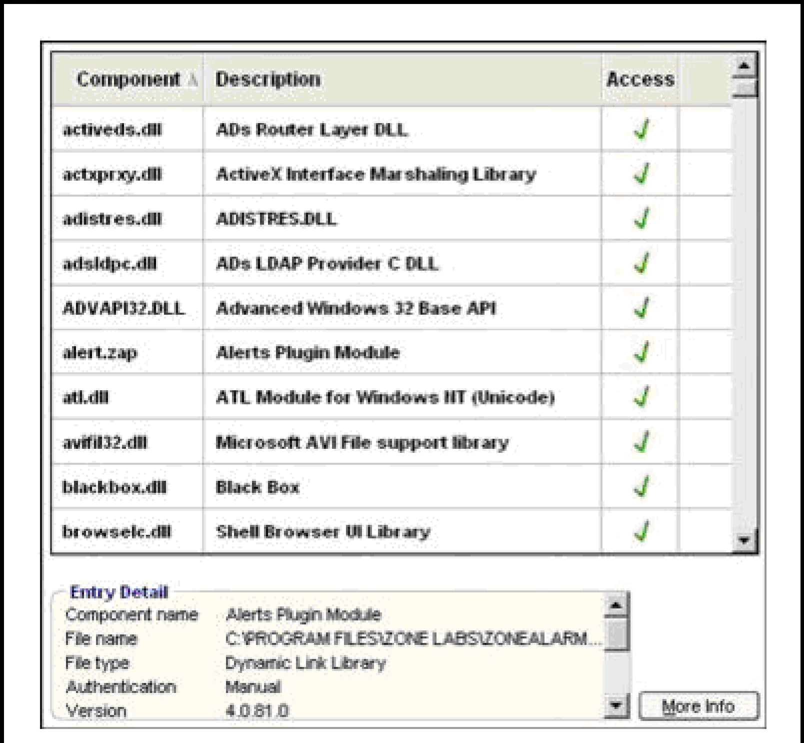
Active	Programs	Smart Defense	Trust Level	Access		Server		Send Mail
				Trusted	Internet	Trusted	Internet	
	Windows Update A...	Auto	?	?	?	?	?	?
	Windows NT Sessi...	Auto	▮▮	✓	✓	?	?	?
	Windows NT Multipl...	Auto	?	?	?	?	?	?
●	Windows NT Logon...	Auto	▮▮▮	?	?	?	?	?
	Windows Managem...	Auto	?	?	?	?	?	?
	Windows Explorer	Auto	▮▮▮	✓	✓	?	?	?
	VMwareUser	Auto	?	?	?	?	?	?
	VMwareTray	Auto	?	✗	✗	✗	✗	?
	VMware Tools Ser...	Auto	?	?	?	?	?	?
	Userinit Logon Appli...	Auto	▮▮▮	✓	✓	?	?	?
	TrueVector Service	Auto	?	✗	✗	✗	✗	?

Entry Detail

Product name	Microsoft(R) Windows (R) 2000 Operating System
File name	C:\WINNT\system32\SERVICES.EXE
Policy	Automatically configured
Last policy update	4/22/2005 11:01:22

Managing program components

The Components List contains a list of program components for allowed programs that have tried to access the Internet or the local network.



Component	Description	Access
activeds.dll	ADs Router Layer DLL	✓
actxprxy.dll	ActiveX Interface Marshaling Library	✓
adistres.dll	ADISTRES.DLL	✓
adsldpc.dll	ADs LDAP Provider C DLL	✓
ADVAPI32.DLL	Advanced Windows 32 Base API	✓
alert.zap	Alerts Plugin Module	✓
atl.dll	ATL Module for Windows NT (Unicode)	✓
avifil32.dll	Microsoft AVI File support library	✓
blackbox.dll	Black Box	✓
browselc.dll	Shell Browser UI Library	✓

Entry Detail

Component name	Alerts Plugin Module
File name	C:\PROGRAM FILES\ZONE LABS\ZONEALARM...
File type	Dynamic Link Library
Authentication	Manual
Version	4.0.81.0

Firewall Configuration

_enD

Firewall techniques

[1] http://www.webopedia.com/TERM/f/firewall.html accessed by (04.06.2006)
[2] http://www.pcmag.com/encyclopedia_term/0,2542,t=firewall&i=43218,00.asp accessed by (04.06.2006)
[3] http://computer.howstuffworks.com/firewall1.htm accessed by (04.06.2006)
[4] http://www.pcmag.com/encyclopedia_term/0,2542,t=firewall&i=43218,00.asp accessed by (04.06.2006)
[4] http://www.pcmag.com/encyclopedia_term/0,2542,t=firewall&i=43218,00.asp accessed by (04.06.2006)
[5]http://www.pcmag.com/encyclopedia_term/0,2542,t=firewall&i=43218,00.asp accessed by (04.06.2006)
[6] http://computer.howstuffworks.com/firewall2.htm
[7] http://www.zonelabs.com/store/content/support/zasc/whyFirewall.jsp?lid=home_pc_firewall accessed by (04.06.2006)
[8] http://www.zonelabs.com/store/content/support/zasc/whyFirewall.jsp?lid=home_pc_firewall accessed by (04.06.2006)
accessed by (04.06.2006)