



August 2001

Revision 1.1

P.O. Box 2266 , 1300 Taylors Lane, N.J. 08077, Cinnaminson U.S.A

Table of Contents :

1. Introduction	
1.1 How do Intruders get into systems	Page 4
1.2 What is Network intrusion detection	Page 4
1.3 How can intruders get into system	Page 5
2. What is Mindwall	Page 6
3. Distinctive features of Mindwall	
3.1 Network Intrusion Detection	Page 7
3.2 Content Scanning / Blocking	Page 8
3.3 Network Monitoring / Logging	Page 9
4. How the Mindwall Works	Page 10
5. Basic operational information about Mindwall	Page 11
5.1 Pre-Installation	Page 11
5.2 After Installation	Page 12
5.3 Creating an event report	Page 15
6. Why do you need Mindwall if you already have a Firewall	Page 16
7. Feature List	Page 17
8. Environment	Page 18
9. Contact Information	Page 19

1. Introduction

The Internet has completely changed the way we work, do business and communicate. Use of Internet has grown and developed beyond all expectations. Developments of new operating systems, hardware and software are continuing at rapid pace. With development of new software, new security vulnerabilities and bugs become surface.

Software always has bugs. System Administrators and Programmers can never track down and eliminate all possible holes. Intruders have only to find one hole to break in.

There are two words to describe the intruder: hacker and cracker. Terms hacker and cracker are generic terms for a person who likes getting into things. The benign hacker is the person who likes to get into his/her own computer and understand how it works. The malicious hacker is the person who likes getting into other people's systems.

Intruders can be classified into two categories :

Outsiders

Intruders from outside your network, attack your external presence (deface web servers, forward spam through e-mail servers, etc.). They may also attempt to go around the firewall to attack machines on the internal network. Outside intruders may come from the Internet, dial-up lines, physical break-ins, or from partner (vendor, customer, reseller, etc.) networks that are linked to your corporate network.

Insiders

Intruders who legitimately use your internal network. These include users who misuse privileges or who impersonate higher privileged users (such as using someone else's terminal). A frequently quoted statistic is that 80% of security breaches are committed by insiders

1.1 How do intruders get into systems?

The primary ways an intruder can get into a system:

Physical Intrusion If an intruder has physical access to a machine (i.e. they can use the keyboard or take apart the system), they will be able to get in. Techniques range from special privileges of the console, to the ability to physically take apart the system and remove the disk drive (and read/write it on another machine). Even BIOS protection is easy to bypass, virtually all BIOSes have backdoor passwords.

System Intrusion This type of hacking assumes the intruder already has a low-privilege user account on the system. If the system doesn't have the latest security patches, there is a good chance the intruder will be able to use a *known exploit* in order to gain additional administrative privileges.

Remote Intrusion This type of hacking involves an intruder who attempts to penetrate a system remotely across the network. The intruder begins with no special privileges. There are several forms of this hacking. For example, an intruder has a much more difficult time if there exists a firewall between him/her and the victim machine.

1.2 What is NIDS?

An intrusion is somebody (known as "hacker" or "cracker") attempting to break into or misuse your system. The word "misuse" is broad, and can reflect something severe as stealing confidential data to something minor such as misusing your email system for spam.

An "Intrusion Detection System (IDS)" is a system for detecting such intrusions.

1.3 How can Intruders get into systems?

Software bugs are exploited in the server *daemons*¹, the client applications, the operating system, and the network stack.

Software bugs can be classified in the following manner:

Buffer overflows: Almost all the security holes you read about in the news are due to this problem.

A typical example is a programmer who sets aside 256 characters to hold a login username. Surely, the programmer thinks, nobody will ever have a name longer than that. But a hacker thinks, what happens if I enter in a false username longer than that? Where do the additional characters go? If they hackers do the job just right, they can send 300 characters, including code that will be executed by the server, and voila, they've broken in.

Hackers find these bugs in several ways. First of all, the source code for a lot of services is available on the net. Hackers routinely look through this code searching for programs that have buffer overflow problems.

Secondly, hackers may look at the programs themselves to see if such a problem exists, though reading assembly output is really difficult.

Thirdly, hackers will examine every place the program has input and try to overflow it with random data. If the program crashes, there is a good chance that carefully constructed input will allow the hacker to break in.

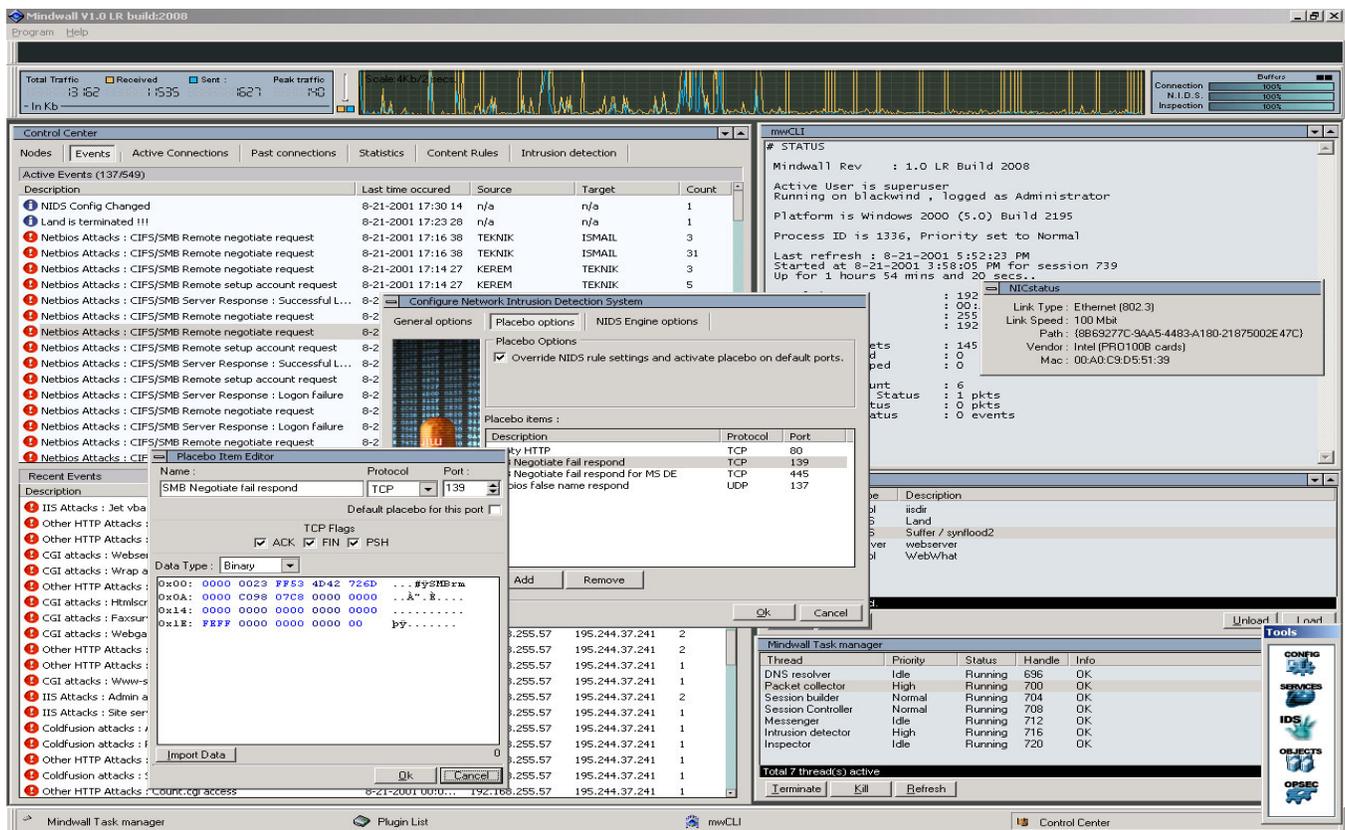
Unexpected combinations: Programs are usually constructed using many layers of code, including the underlying operating system as the bottom layer. Intruders can often send input that is meaningless to one layer, but meaningful to another layer. The most common language for processing user input on the web is PERL.

Programs written in PERL will usually send this input to other programs for further evaluation. A common hacking technique would be to enter something like "l mail < /etc/passwd". This gets executed because PERL asks the operating system to launch an additional program with that input. However, the operating system intercepts the pipe '|' character and launches the 'mail' program as well, which causes the password file to be emailed to the intruder.

Unhandled input: Most programs are written to handle valid input. Most programmers do not consider what happen when somebody enters input that doesn't match the specification.

Race conditions: Most systems today are "multitasking /multithreaded". This means that they can execute more than one program at a time. There is a danger if two programs need to access the same data at the same time. Imagine two programs, A and B, who need to modify the same file. In order to modify a file, each program must first read the file into memory, change the contents in memory, then copy the memory back out into the file.

The race condition occurs when program A reads the file into memory, then makes the change. However, before A gets to write the file, program B steps in and does the full read/modify/write on the file. Now program A writes its copy back out to the file. Since program A started with a copy before B made its changes, all of B's changes will be lost. Since hackers need to get the sequence of events in just the right order, race conditions are very rare. Intruders usually have to try thousands of times before they get it right and hack into the system.



2. What is Mindwall ?

Mindwall is an advanced network security system. It is a combined software that provides you with information, alerts and controls to protect your system from external attacks and intrusions, and internal abuses.

Mindwall's Major features are:

Network Intrusion Detection System (NIDS)

Mindwall's NIDS module monitors the network and server activity to detect malicious attempts such as denial service attacks, unauthorized access and reconnaissance attacks. When the Mindwall's NIDS module detects such activity, it responds with variety of ways including logging the attack, responding with countermeasure packets, informing the administrator and the terminating the attack immediately. At the present time, there are more than 700 NIDS (Network Intrusion Detection System) rules in its database which is enabling Mindwall to detect more than 2000 attacks.

Because of modular infrastructure those operations are done without blocking the analysis of incoming & outgoing traffic. Mindwall's unique IDS rule editor enables our users to define their own intrusion detection rules easily.

Connection Scanning / Blocking

Mindwall can act like a firewall; you can block sites or block certain service usages such as *irc* or *web*. You can also define content-based rules like non-productive site blocking rules.

The administrator can block or override any existing connection on the network

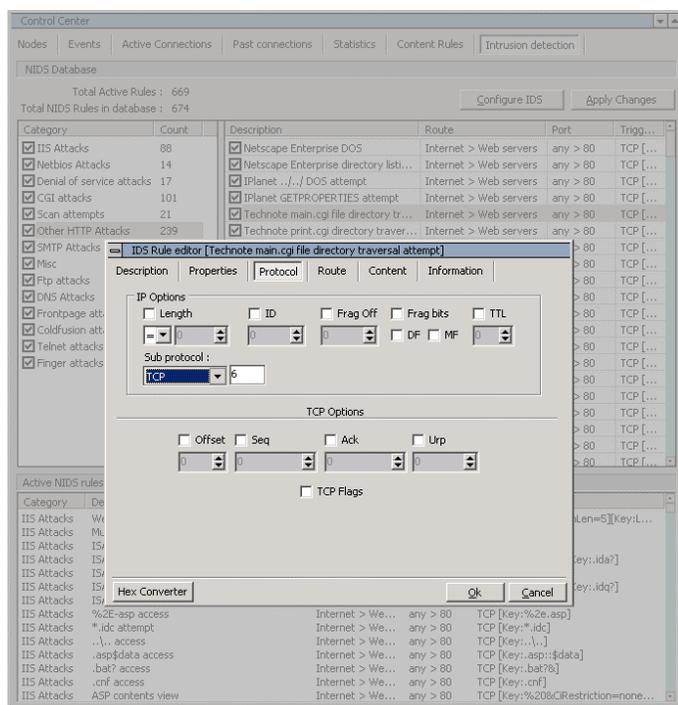
Network Monitoring

Mindwall has an advanced network-monitoring module that allows you to view active TCP/UDP sessions on your network. It has many filtering options (like email, web, hexadecimal) to ease viewing of the connection content. It also has a service based logging mechanism (cryptal) to log sessions according to their content.

3. Distinctive features of Mindwall

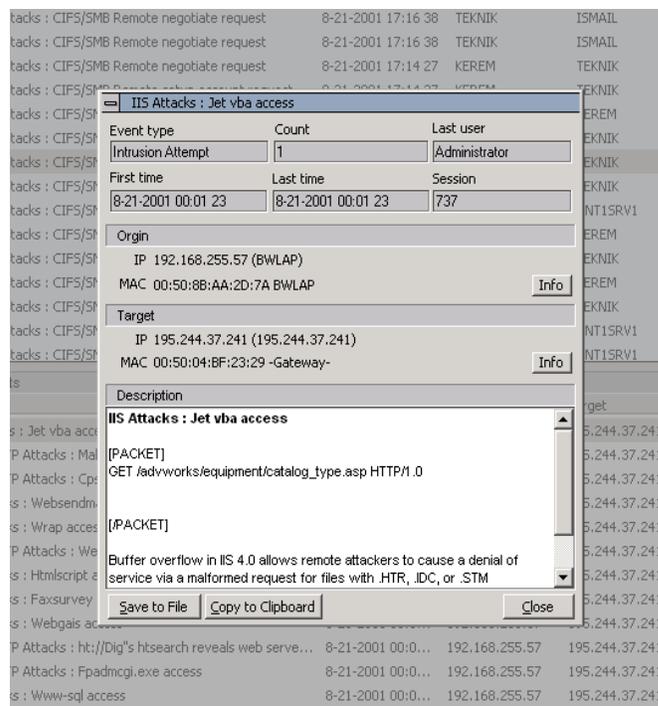
3.1 Network Intrusion Detection System (NIDS)

Mindwall can detect intrusions such as exploit attacks, denial-of-service (DoS) and reconnaissance attacks in *real time*. It's intrusion detection engine scans every incoming and outgoing packet. This scanning process is done in *stealth*, remaining undetectable to attackers. Intruders are often caught unaware as they don't know they are being monitored and logged.



The Intrusion detection engine has both internal and external rules for detecting attacks. Predefined rules can detect wide range of attacks. Currently Mindwall has more than 700 predefined NIDS rules in its database and more than 100 internal rule to detect complex attacks.. The Administrator can define his/her own intrusion detection rules.

NIDS Rules are highly categorized with their type and compromise levels. Mindwall has configuration options to enhance reaction performance.



As well as detecting/logging incoming attacks, Mindwall can block incoming attacks.. The Intrusion logging system is linked to Mindwall's common event subsystem. Mindwall generates a special event record for every intrusion or unusual event and It saves its event records to its database constantly. Every intrusion event item contains many critical information such as Source and Destination MAC, IP addresses, protocol fields, Event start and finish time and attack counter and the contents of packet.

Placebo System

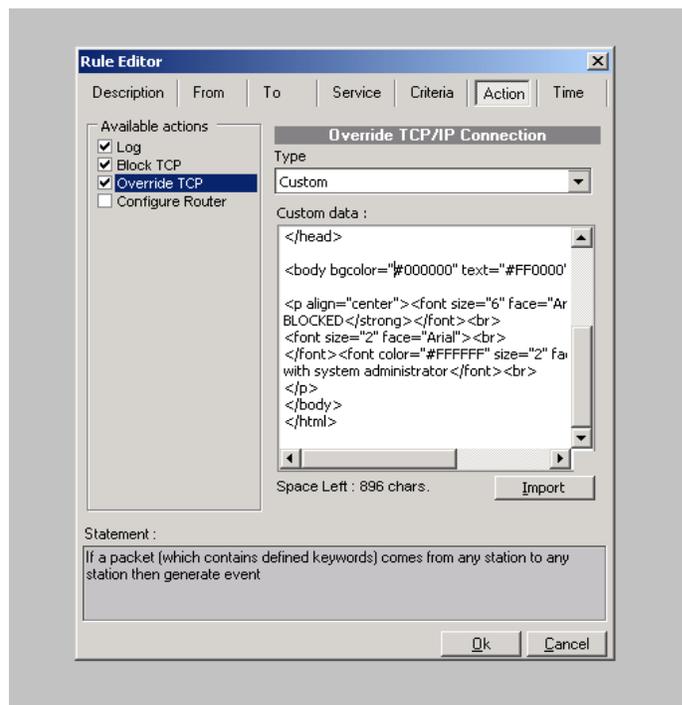
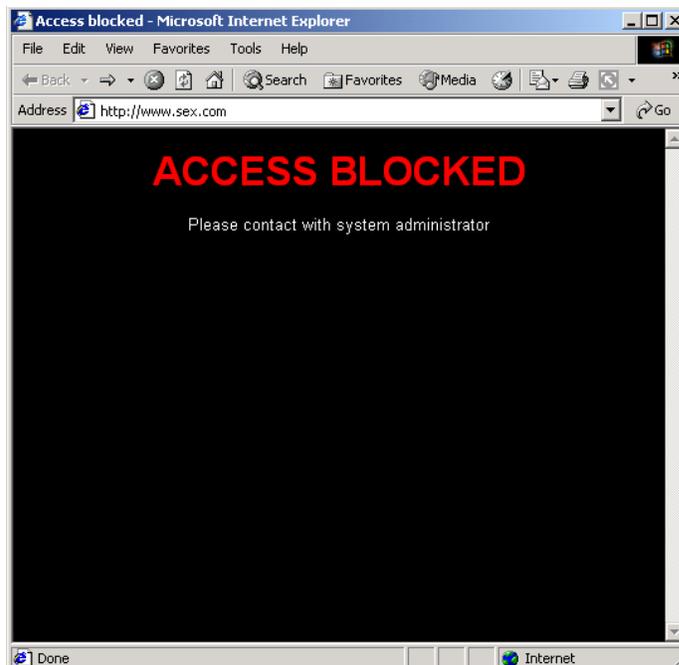
Mindwall also has a unique feature called Placebo system which is used for responding the attack with counter-measure packets. It is used for distracting attacker to have more information about attacker and the attack. Placebo system works as a part of NIDS system and it's being triggered instantly when an attack detected. Placebo system's behaviour can be configured to give unique responses against various attacks.

3.2 Connection Blocking

Mindwall can act like a firewall; It can block established connections and connection request's. Our product listens to every connection from the beginning and collects connection's TCP₁ ACK₂ and SEQ₂ numbers . With those numbers Mindwall can virtually block every TCP connection by sending spoofed packets to both server and client with FIN₃ / RST₃ flag. Our clients can create rules to block IP addresses or block certain service usages such as ICQ or IRC. Group definitions ,IP masks and *Hosts lists* are available to ease the creation rules. Defining content , keyword and binary data based rules is also possible. Mindwall can block or override any existing connection on the network or re-configure the router for desired action. Mindwall has several alert tools to warn the system administrator on necessary situations.

With this feature, it is possible to block web sites with nonproductive or unwanted content. Also website ratings can be implemented to our rule system by entering rating keywords to blocking rules.

This feature of Mindwall enables system administrators to log or block connections to external networks with data containing your commercial secrets. Mindwall also has a customized connection overriding (*connection hijacking*) feature which is very useful tool to intervene , terminate or block any active connection in intrusion attempt.



- (1) TCP stands for Department of Defense standard Transmission Control Protocol , which is most widely used Internet protocol.
- (2) SEQ and ACK numbers are the reliability and flow control values of TCP/IP protocol.
- (3) TCP/IP Protocol uses flags to indicate the operation for packet . Flags FIN(Finalize) and RST (Reset) indicates end of connection.

3.3 Network Monitoring / Logging features

Mindwall has 4 different logging and monitoring approach
These are:

Service depended connection Logging

Content based traffic logging

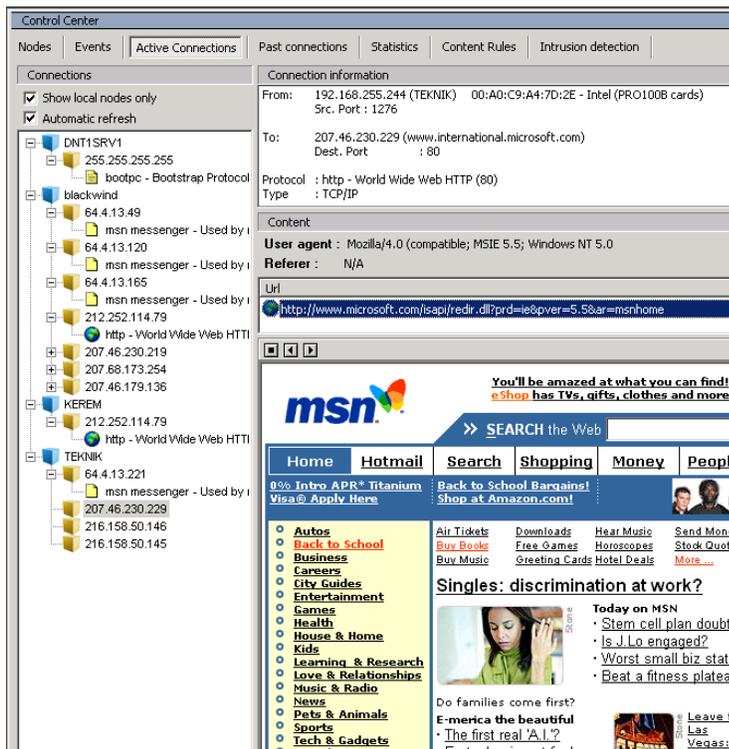
ARP Traffic monitor

Network graphic

Protocol distribution chart

3.3.1 Connection Monitoring / Logging

Our Application simulates each connection on the network internally depending on incoming/outgoing traffic. Instead of millions of low level packets, the administrator sees the connection content just like the client sees.

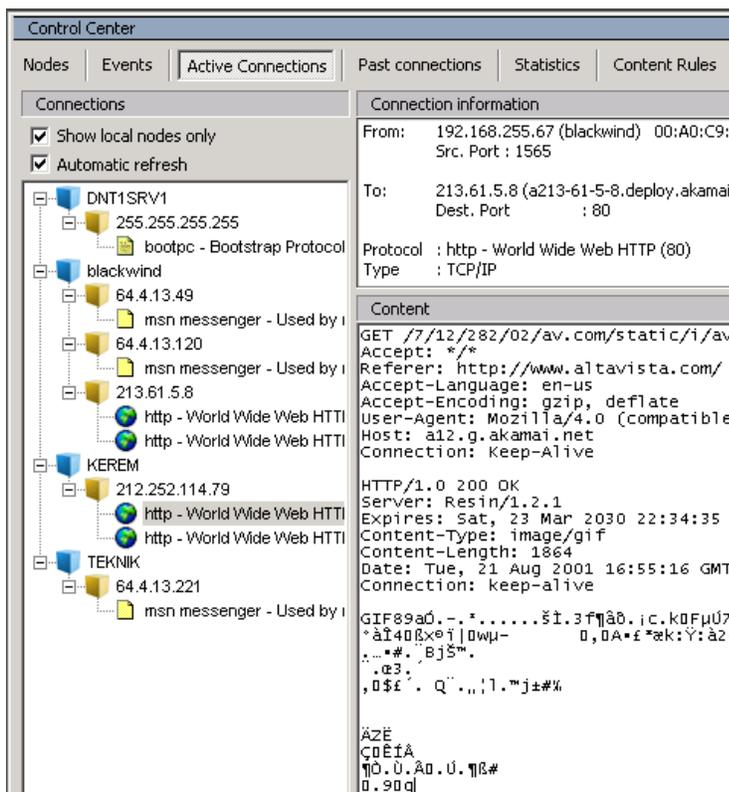


Mindwall constructs 3 different (Server based, client based, protocol based.) *connection tree* to ease viewing of active connections. This is a very powerful tool to view and administrate active connection based traffic on network. Most administration functions of Mindwall can be accessed by left clicking a host in *connection tree*.

Mindwall also has textual, hexadecimal and http filters to ease viewing of connection content. These filters are highly configurable for advanced monitoring purposes.

3.3.2 Content based traffic logging

Mindwall can be configured to log connections with specific content by adding rules .



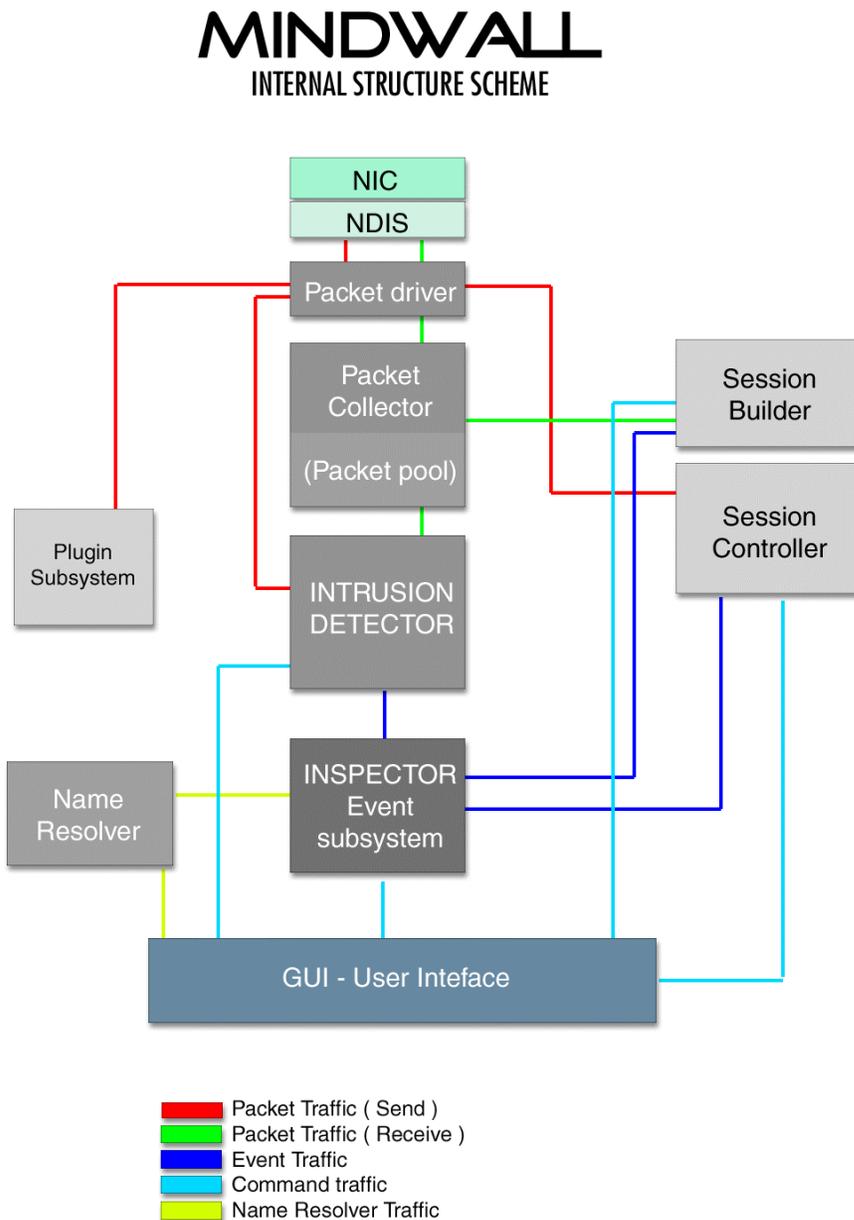
4. How the Mindwall works ?

Mindwall uses *NDIS*¹ to capture packets from network interface. It supports *ethernet 802.3 interface protocol*, however its infrastructure is designed to support other network layer protocols such as *ATM*. Packet capture driver is used to switch the network interface card to *promiscuous* mode. A module named "*Packet collector*" captures packets from *NDIS* driver, then collects them into a *Packet Pool*.

Intrusion detection module uses this packet pool to analyze packets, *Session builder* uses packet pool to rebuild connection for monitoring purposes, *Session controller* checks packets and connection table to execute Custom Network Rules. We also have a thread named *Name Resolver* to resolve ip addresses. *Session builder module* virtually creates the existing connections by analyzing the incoming packets and saves them using database engine. *Session Controller* module also checks connections for complex attacks using internal IDS rules. For utilising processing power and minimize packet loss, each thread has its buffering mechanism. There is another thread for refreshing GUI. It has the lowest priority of the application ,

Mindwall's Blocking feature and the Placebo System uses *Spoofed packets*. To terminate connection, Mindwall sends both sides (Client / Server) spoofed IP packets with RST or FIN with correct SEQ , ACK numbers. Mindwall acquires those numbers by listening to each connection on network. Blocking feature of Mindwall requires no packet loss . Also Mindwall has unique feature called 'Placebo System' which is used for attack counter - rmeasure purposes.

(1) *NDIS* is short for the "*Network Driver Interface Specification*". *NDIS* provides a library of functions that can be used by *MAC (Media Access Controller)* drivers as well as higher level protocols (such as *TCP/IP*).

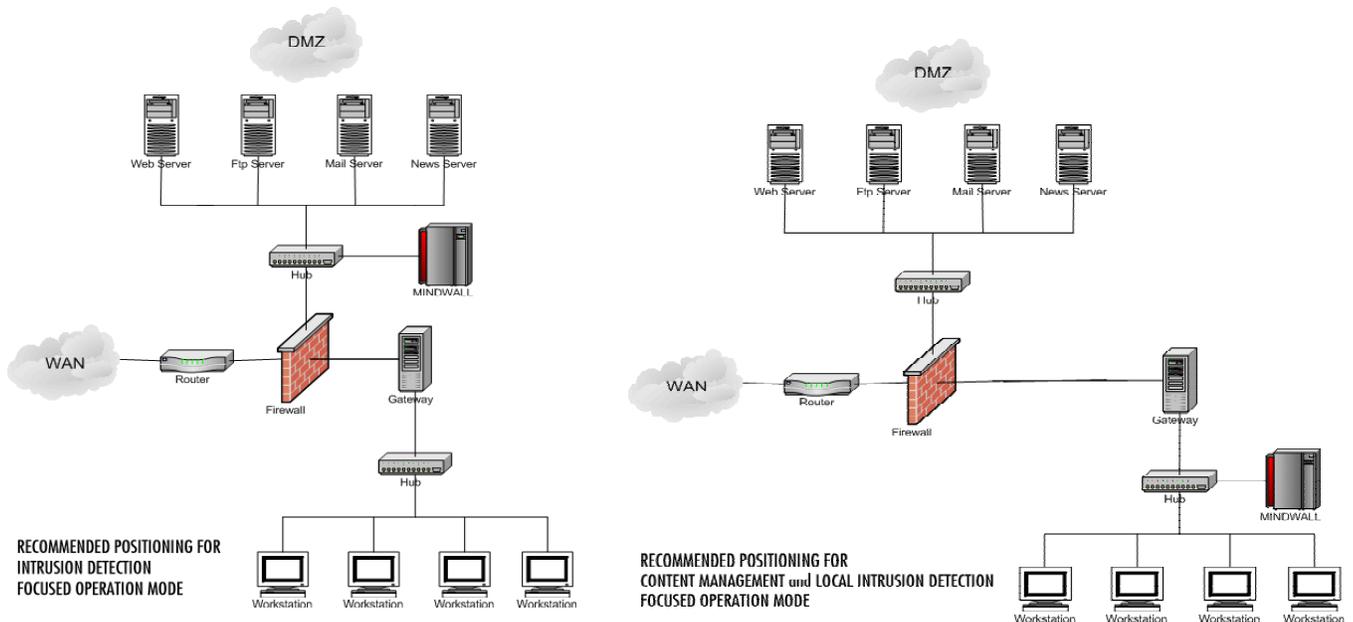


5. Basic Operational instructions for Mindwall

5.1 Pre-Installation

- Positioning the Mindwall

Mindwall requires to be at correct location to fully perform its functions. See following figures for necessary positioning for certain operation modes.



- IP related issues.

Mindwall will have problems detecting gateway and other TCP/IP related information on DHCP or other dynamic IP assigned systems. Switch to static ip addressing on local machine.

- Pre-Installed applications

Any kind of network related software such as firewalls , Intrusion detection software's or any other application which is using NDIS/TDI driver on local machine may cause Mindwall to fail on certain operations. Uninstall all network related software on local computer including server applications.

- **Driver issues**

Packet driver installation is required for Mindwall to operate. Installer will auto-install Mindwall's default packet driver. However, if you have specific hardware, you may want to install NIC specific NDIS driver which can be obtained from our website before installing.

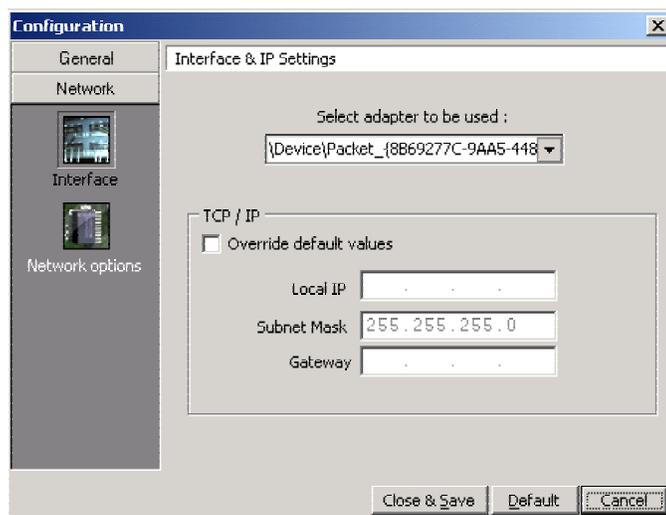
5.2 After Installation

Mindwall requires to be configured properly to operate. Following configuration options should be verified before defining rules and activating placebo system and active intrusion detection.

- **Driver Selection**

Mindwall can be configured to use different interfaces by using Interface and IP settings dialog on configuration dialog which can be accessed through both application menu and Shortcut Toolbar on main window. Click on Combo box under the text 'Select adapter to be used' to change the active adapter that Mindwall is using. After making necessary changes, restart the application.

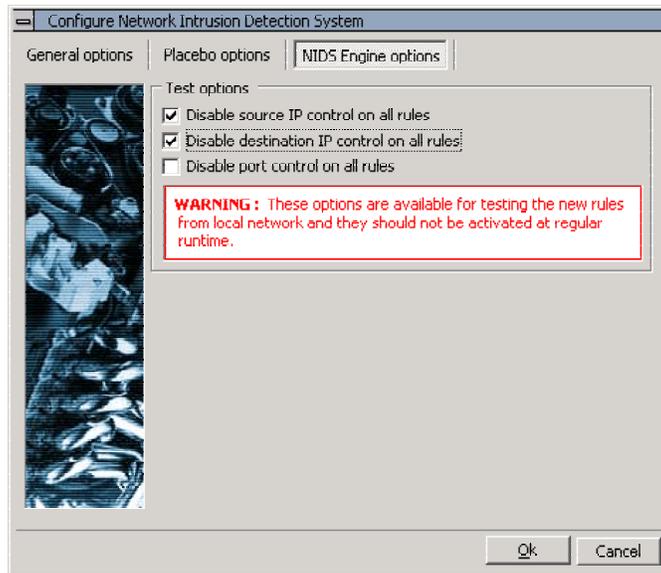
Make sure that Mindwall is using correct NIC interface.



- **Configuring the NIDS Engine**

Most of the NIDS rules in Mindwall will check for route of incoming packet before analyzing its content. You may want to disable route check for testing purposes to configure Mindwall to ignore this route checking. You can access this dialog by pressing 'Configure IDS' button on the Intrusion detection Tab on Control Center window.

Please note that these options are for testing purposes and should not be activated in regular runtime. You may want to disable netbios and other rule groups before disabling route check. De-activating route check may cause Mindwall to assume local traffic as intrusion.

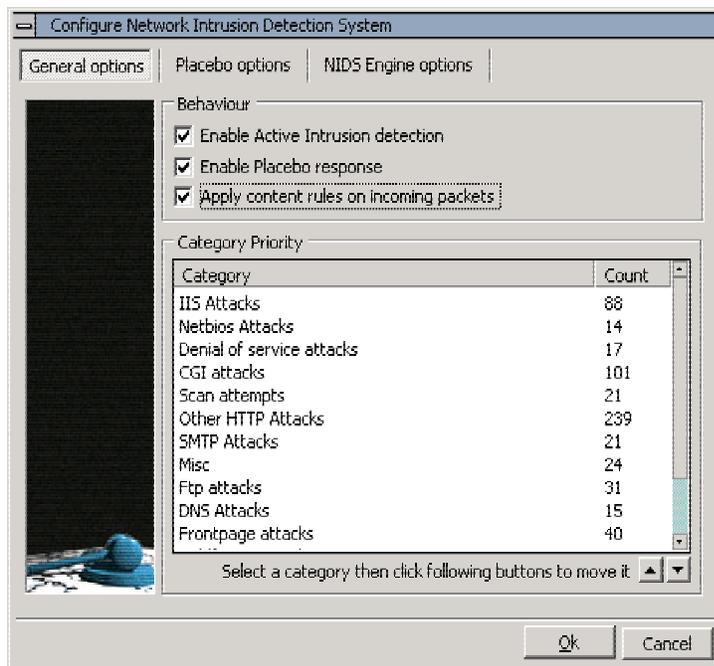


- **Activating 'Active Intrusion detection' And Placebo System**

By default Mindwall will only report intrusions. To activate 'Active Intrusion Detection System' you must configure Mindwall by pressing Configure IDS button on Intrusion Detection Tab on Control Center window.

This dialog contains another option called 'Apply content rules on incoming packets', This option will tell Mindwall to double check content rules by inserting Content rules to NIDS Engine.

Category Priority on this dialog is for configuring the priority of defined rule sets. You can prioritize desired category by pressing up and down buttons after 'Select a category then click following buttons to move it' text.

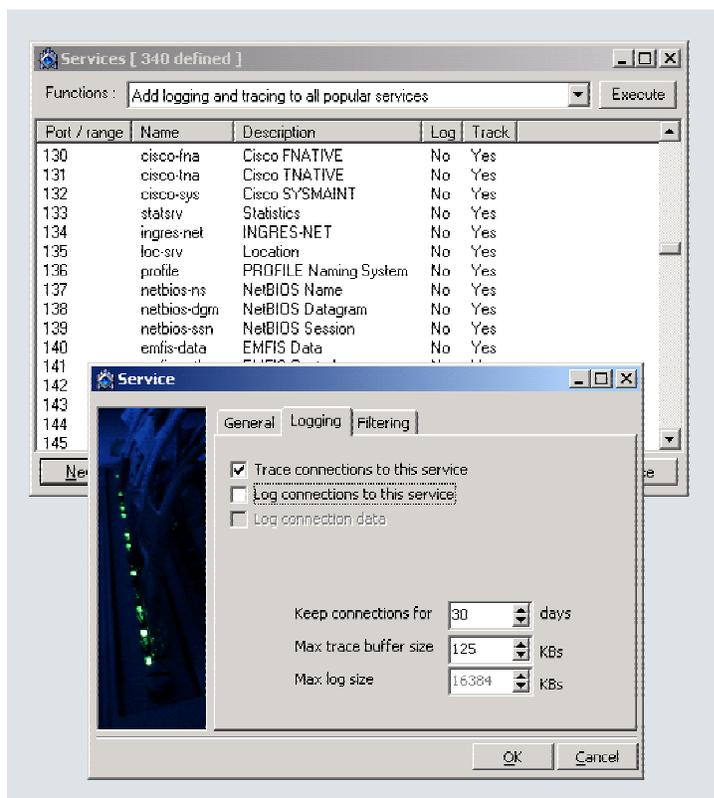


- **Verifying Services to be monitored and Logged**

By Default Mindwall will monitor & Log almost all ports, If you have intense traffic on your network, you should deactivate monitoring of some services to get better performance results.

To Configure Service options, click on Services menu then Select desired service then click logging tab and select or deselect 'Trace connections to this service' or 'Log connections to this service'. You can also access Services window by clicking

You may also disable logging and tracing of all services to increase Intrusion detection performance.



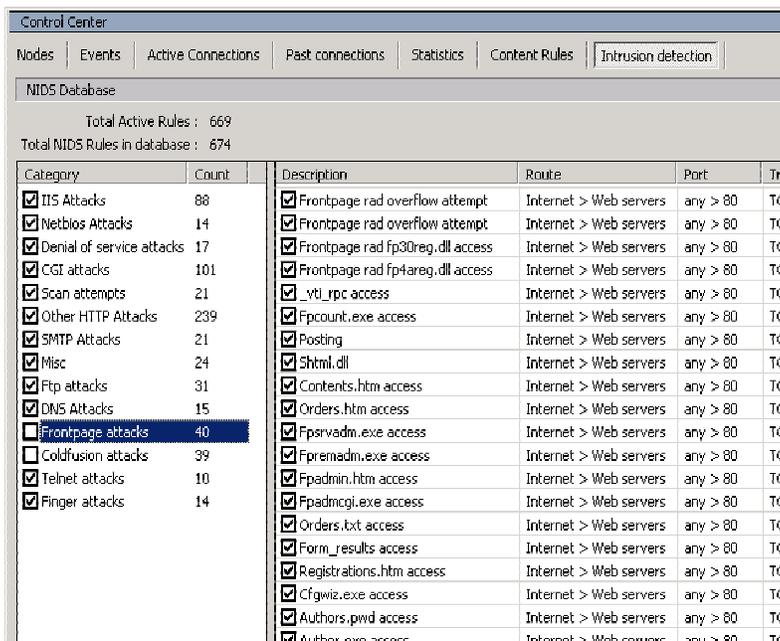
- **Selecting IDS Rule groups to be used by Intrusion Detection Engine**

To Increase overall performance and response time , you should disable IDS Rule Categories that doesn't apply to your network For example you may want to disable Coldfusion IDS Rule Category if you don't have Coldfusion applications on your network. By doing so you will increase response time of Mindwall and eliminate possible TCP Blocking / Placebo system latency problems.

You can also disable a rule that doesn't apply to your network even if its in a Category which is Active.

To See Rule Categories, press Intrusion Detecion tab on Control Center Window , To activate de-activate Category Click on checkbox before name of rule category..

After making changes to NIDS Database , press Apply Changes button. Mindwall will immediately probe NIDS engine to stop and get new IDS Rule configuration.

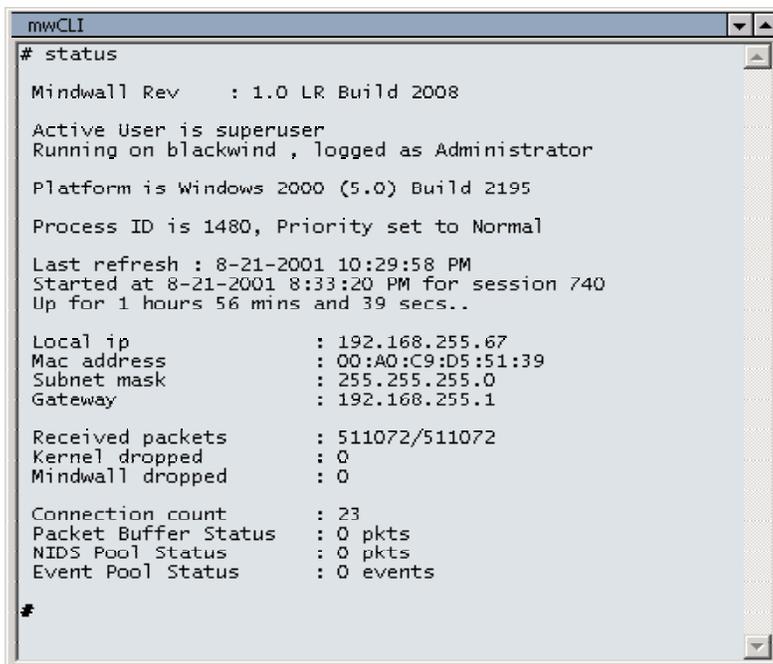


- **Checking IP Configuration**

Type Status at mwCLI window to see several configuration information such as Local IP , MAC address information , Subnet mask (which is used for detecting local network) , Gateway IP.

Make sure that Mindwall has detected proper IP Configuration settings.

You may change IP configuration from Windows TCP/IP Options or you can use Network options under configuration window to override default configuration variables.



5.4 Creating Event Report

Mindwall will create an event for every network intrusion, unusual activity .

These events are categorized as

Active events (Event list which contains event information for occurred on active session)

Recent events (Event list which contains event information for past sessions)

You can get a report of both recent and active events. To do this, press left click on Event window and select Create Report . Mindwall will prompt you for a file name , you can use default filename . After giving file name , Mindwall will create html detailed report of events.

Mindwall Event Report

Created at 8-21-2001 / 3:58:21 PM with Mindwall V1.0 LR b2008
www.mindwall.com

Sessions

[Session 738](#) [Session 737](#) [Session 736](#) [Session 735](#)

Events

- Session 738 -

[Go Top](#)

Mindwall shutdown for session 738

Event Type	Mindwall event
Event Date	8-21-2001
Event Time	1:27:38 AM

Netbios Attacks : CIFS/SMB Remote negotiate request

Event Type	Intrusion Attempt
Event Date	8-21-2001
Event Time	First : 1:19:33 AM Last : 1:27:02 AM
Origin	192.168.255.67 [192.168.255.67]
Target	192.168.255.57 [192.168.255.57]
Source MAC	00:AD:C9:D5:51:39 [192.168.255.67]
Target MAC	00:50:8B:AA:2D:7A [192.168.255.57]
Count	2

```
[PACKET]
..\\SMB\\SEYbbPC NETWORK PROGRAM 1.0\LANMAN1.0\Windows for Workgroups 3.1a\LM1.2X002LANMAN2.1\NT LM
0.12
[/PACKET]
```

This event indicates that a remote attacker attempted to establish netbios connection via TCP

IIS Attacks : cmd.exe access

Event Type	Intrusion Attempt
Event Date	8-21-2001
Event Time	1:26:46 AM

6. Why do you need Mindwall if you already have a Firewall

A common misunderstanding is that firewalls recognize attacks and block them. This is not true.

A Firewall is simply a device that shuts off everything, then turns back on only a few well-chosen items. In a perfect world, systems would already be "locked down" and secure, and firewalls would be unneeded. The reason we have firewalls is precisely because security holes are left open accidentally. Thus, the first thing a firewall does is stop ALL communication.

The firewall administrator then carefully adds "rules" that allow specific types of traffic to go through the firewall. For example a typical corporate firewall allowing access to the Internet would stop all UDP and ICMP datagram traffic, stops incoming TCP connections, but *allows* outgoing TCP connections. This stops most incoming connections from outside, but still allows internal users to connect in the outgoing direction.

A firewall is simply a fence around your network, with a couple of well chosen gates. But a fence has no capability of detecting somebody trying to break in (such as digging a hole underneath it), nor does a fence know if somebody coming through the gate is allowed in. It simply restricts access to the designated points.

For example, in April of 1999, many sites were hacked via a bug in ColdFusion. These sites all had firewalls that restricted access only to the web server at port 80. However, it was the web server that was hacked. Thus, the firewall provided no defense. On the other hand, an intrusion detection system would have discovered the attack, because it matched the signature configured in the system. Another problem with firewalls is that they are only at the boundary to your network. Roughly 80% of all financial losses due to hacking come from inside the network. A firewall at the perimeter of the network sees nothing going on inside; it only sees that traffic which passes between the internal network and the Internet.

In summary, a firewall is not the dynamic defensive system that users imagine it to be.

Some reasons for adding MINDWALL to your network

- *Catches attacks that firewalls legitimate allow through (such as attacks against web servers).*
- *Blocks attacks*
- *Detects / Logs Misuse of networks.*
- *Catches hacking attempts that fail.*
- *Catches insider hacking.*
- *Double-checks mis-configured firewalls.*

7. Feature list

Intrusion detection

Active Intrusion Detection System

Attack Countermeasure feature (Placebo)

Intrusion Detection Database

Detecting intrusions, attacks, trojan's and other malicious attempts

Detecting suspicious network events

Monitoring

Monitoring and logging of network activity.

Advanced connection logging mechanism

Performing or invoking actions when certain events occur.

Blocking unwanted activities.

Network Traffic diagram and protocol distribution reports.

Detecting users connecting to specific sites.

Detecting users using specific protocols.

Detection of connections that includes specific keywords.

Event logging mechanism

Network Administration

mwCLI - Unix like command line interface for plugin files or internal commands.

Packet Counters - Packet and traffic information tool

Host Information - Detailed host information utility

Infrastructure

Task management system

Software development kit (available for Delphi and Visual C++)

Plugin subsystem for all modules

MAC Address based operations.

8. Environment

Mindwall runs on following operating systems :

Windows NT 4.0

Windows 2000 Server Edition

Windows 2000 Professional Edition

Minimum System Requirements :

Pentium III 800 or higher processor speed.

256Mbyte RAM

High speed disk drive with more than 1 GB Disk space.

Ethernet Interface

9. Contact Information

Contact

Please contact us in the U.S. at (856) – 864 - 0115 or e-mail to info@priority1world.com. Please include your name, e-mail address and company name along your inquiry. Visit us at www.priority1world.com or www.mindwall.com for additional information such as downloads, additional screen shots, demonstrations and frequently asked questions

Priority 1
Software Solutions, LLC.
P.O. Box 2266
1300 Taylors Lane,
N.J. 08077, Cinnaminson
U.S.A

Phone : (856) 864 - 0115
Fax : (856) 829 - 9203

Testimonials

Feedback from our clients is very important to us. Please forward your comments and experience with Mindwall or Testimonials to testimonials@priority1world.com

© Copyright 2001 Priority 1 Software Solutions LLC . All rights reserved.

Mindwall and Mindwall logos are the trademark of Priority 1 Software solutions LLC.

All trademarks and service marks in this document are the property of their respective owners.
No information on this document may be copied or reproduced in any form without the express written consent of Priority 1 LLC.