1. Firewall Configuration

A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

Advanced Options: This section contains options for protecting against particular wellknown attacks as well as documenting those attacks as they occur.

Firewall Databases: This section allows you to create groups based on IP addresses, subnet masks, ports, and time. These groups are used when creating inbound and outbound policies.

Inbound/Outbound Policies: This section allows you to create rules for incoming and outgoing IP packets. The IP packets are compared against the rules and are allowed or denied accordingly.

Firewall Enable/Disable: This option enables/disables all the protection provided on these pages.

1.1 Protection Policy

Protection Policies defend against common methods of attacking a network and computers within the network. Some of these attacks are classified as a DoS (Denial of Service). DoS is an attack in which a network or components of a network are disabled, usually by overloading traffic on the network, in order to prevent authorized and legitimate users to access network resources.

Basic Protection:

• **IP Spoofing checking:** IP spoofing is when an unauthorized user inserts the IP address of an authorized user into the IP packets in order to gain access to a network. Selecting this option will allow the firewall to check for and filter out this discrepancy.

• **Ping of Death checking:** Ping of Death is a type of DoS attack that uses a malformed ICMP data packet that contains unusually large amounts of data that causes TCP/IP to crash or behave irregularly. Enabling this will allow the firewall to filter out packets containing Ping of Death properties.

• **Land Attack checking:** Land attack is a type of DoS attack that works by sending a spoofed packet containing the same source and destination IP address and port (the victim's IP address). This packet contains a connection request, resulting in a handshake process. At the end of the handshake, the victim sends out an ACK (ACKnowledge) request. Since the source and the destination are the same, the victim receives the ACK request it just sent out. The received data does not match what the victim is expecting, so it retransmits the ACK request. This process repeats until the network crashes. Enabling this will allow the firewall to filter out possible Land Attack packets.

• **Reassembly Attack checking:** Reassembly Attack is a type of DoS attack that exploits the weakness of the IP protocol reassembly process. As discussed earlier in this user guide, packets undergo fragmentation when they exceed a certain maximum size. Certain criteria define the packet fragmentation process so that packets can be reassembled properly. In Reassembly Attack, the subpackets have malformed criteria (fragment offset), which can easily cause a system to crash, freeze, or reboot. Enable this option to check for and filter out Reassembly Attack packets.

Advanced Protection:

• **SYN Flooding checking:** SYN Flooding is a type of DoS attack that is accomplished by not sending the final acknowledgement to the receiving server's SYN-ACK (SYNchronize-ACKnowledge) in the final part of the handshake process. This causes the serve to keep signaling until it is timed out. When a flood (many) of these attacks are sent simultaneously, the server will probably overload and crash. Enable SYN Flooding checking to filter out possible SYN flood packets.

• **ICMP Redirection checking:** Also known as an ICMP storm attack or smurf attack, ICMP Redirection is another form of DoS. This attack is performed by sending ICMP echo requests to a broadcast network node. The return IP address is spoofed and replaced by the victim's own address, causing it to send the request back to itself. This causes the broadcast address to send it out to all the network nodes in the broadcast area (usually the entire LAN). In turn, all those recipients resend it back to the broadcast. The process repeats itself, gaining more amplitude through each iteration and eventually causing a traffic overload and crashing the network. Enable ICMP Redirection checking to filter out packets containing the threat.

• **Source Routing checking:** Source routing gives the sender of a packet the ability to determine the exact route that an IP packet takes to get to the destination. However, source routing can be used for malicious reasons. Using a source routed packet, the sender could find out important information about nodes in a network, making it easy to exploit any weakness. Enabling Source Routing checking will cause the firewall to filter out any packet with Source Routing properties.

• **WinNuke Attack checking:** WinNuke exploits a large networking bug found in Windows 95 and NT. WinNuke sends erroneous OOB (Out-of-Band) data that Windows is unable to process, causing the target computer to crash. Enable this if you are running an early (95 or NT) version of Windows that is vulnerable to this attack.

1.2 Hacker Log

This page allows you to configure which Protection Policy (see previous section) violations to log for admin viewing.

Alert Log: Enable/Disable for SYN Flooding, Ping of Death, IP Spoofing, and Win Nuke (all of these are explained in the previous section). Enable to log violations of individual policies.

General Log:

• Deny Policies: Enabling this will add Deny Policy violations to the log. Deny Policies are discussed later in the Inbound/Outbound policy section.

- Allow Policies: Enabling this will add Allow Policy acceptances to the log. Allow Policies are discussed later in the Inbound/Outbound policy section.

Log Database Properties:

- Log Frequency: This field lets you specify how many records to keep of each event. Default is 100. Range for Log Frequency Field is 1-65535.

1.3 Service Filtering

Service Filtering allows you to disable service requests from certain sources. These are the Service Request sources that can be disabled:

- **Ping from External Network**

- **Telnet from External Network**

- **FTP from External Network**

- **DNS from External Network**

- **IKE from External Network**

- **RIP from External Network**

- **DHCP from External Network**

1.4 IP Group

The IP Group lets you specify IP Addresses (Single or Range) and Subnet Masks and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

IP Entry Name: This is the name you assign to the group of IP addresses and subnet masks. The IP Entry Name can be up to 19 characters.

IP addr. 1: This is the IP address or subnet mask you are specifying when creating a group.

IP addr. 2: This field is only active if you select to group a range of IP addresses or subnet masks, in which case this is the end address of that range whereas the IP addr 1 is the first address of that range.

IP/Mask: This field allows you to specify the address type assigned to the group.

- Single IP: This will let you specify one IP address for a given group.

- IP Range: This will let you specify a range of IP addresses for a given group, starting with IP addr 1 and ending with IP addr 2.

- Subnet Mask: This will let you specify a range of subnet masks for a given group.

1.5 Service Group

The Service Group lets you specify a Port and assign it to a group name for easy use when configuring inbound and outbound policies for the firewall.

Service Entry Name: This is the name you assign to the group containing the port number. The Service Name Entry can be up to 19 characters.

TCP/UDP: This specifies whether the port goes through TCP or UDP.

Port #: This is the port number associated with the group name. Range for Port # is 1 – 65535.

1.6 Time Window

The Time Window lets you specify certain time periods and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

Time Window Name: This is the name you assign to the group that is given the time designation. The Time Window Name can be up to 19 characters.

Time Period: This field allows you to specify the time period for both start time and end time by selecting the day, hour, minute, and AM/PM.

1.7 Inbound Policy

The Inbound Policy allows you to filter inbound (from the WAN into the user side LAN) packets based on a set of rules. This enables you to deny access from different sources and thus increase security. A table of inbound policies is displayed with the following information. If there are no policies, then a message stating "*No Entries in Inbound Policy Database*" will be displayed in place of the table.

IP Address: This field specifies the IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.

Port #: This field specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.

Prot.: Short for protocol, this is the protocol to which the policy applies.

Act.: Short for action, this field specifies two possible actions: allow or deny.

Opt. Filtering: Optional Filtering field specifies the time period to which the policy applies.

Up: Clicking this button will move the corresponding policy up one space in the table.

Dn: Short for down, clicking this button will move the corresponding policy down one space in the table.

Note: The Inbound Policy works in a Top-Down fashion according to the Inbound Policy Table. This means that the firewall will apply the policies in order from the top of the table to the bottom. It is critical for both security and user accessibility to the WAN to have inbound policies in the correct order. See Section 1.9.1 for an example of this.

Edit: Clicking this button will display a table similar to the add table (see below) to the bottom of the policy table that will allow you to modify the corresponding policy.

Delete: This will delete the corresponding policy.

Add Inbound Policy: Clicking this button will bring up a table with all the add configurations as shown below:

Src IP: This specifies the Source IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and Subnet Masks that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu. The dropdown menu has four options:

- **Any IP**: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.

- **Single IP**: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

- **IP Range**: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.

- **Mask Range:** Selecting this will enable you to select a range of Subnet Masks to which the policy will apply. The first Subnet Mask in the range must be entered into the first IP Address entry field and the last Subnet Mask in the range must be entered into the second IP Address entry field.

Dest IP: This specifies the Destination IP for the Inbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. See **Src IP** above for configuration detail.

Src Port: This specifies the Source Port for the Inbound Policy. This is the external (WAN side, outside of the firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

- **Any Port:** Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

- **Single Port:** Selecting this will cause only one Port to be affected by the policy. This Port will need to be specified by the user in the first Port entry field.

- **Port Range:** Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

- **Safe Ports:** Any port greater than 1024 (1025 – 65535) is considered a safe port.

Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (LAN side, behind the firewall) Port that will be affected by the policy. See **Src Port** above for configuration detail.

Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

Filtering Action: This specifies what action the policy takes:

- **Allow:** Selecting this will cause the policy to allow packet transfer from the **Src**

IP through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

- **Deny:** Selecting this will cause the policy to deny packet transfer from the **Src**

IP through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

Time Window Filtering: This field allows you to select a certain time frame from the

Time Group in which this policy will be active. See section 6.6 for more information on Time Groups.

DB: Short for Database, this field allows you to select a user-defined IP Group for the**Src IP** and **Dest IP** fields and a user-defined Service Group for the **Dest Port**. User-defined IP and Service Groups are created in **IP Group** and **Service Group** pages.

Note: Source and Destination IP Addresses, Subnet Masks, and Ports are reversed

between Inbound Policy and Outbound Policy. For Inbound Policy, the source

is on the WAN side and the destination is on the LAN side. For Outbound policy,

the source is on the LAN side and the destination is on the LAN side.

1.8 Outbound Policy

The Outbound Policy allows you to filter outbound (from the user side LAN to the WAN) packets based on a set of rules. This enables you to deny access to different sources and thus increase security. A table of outbound policies is displayed with the following information. If there are no policies, then a message stating “No Entries in Outbound Policy Database” will be displayed in place of the table.

IP Address: This field specifies the IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.

Port #: This field specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.

Prot.: Short for protocol, this is the protocol to which the policy applies.

Act. Short for action, this field specifies two possible actions: allow and deny.

Opt. Filtering: Optional Filtering field specifies the time period to which the policy applies.

Up: Clicking on this button will move the corresponding policy up one space in the table.

Dn: Short for down, clicking on this button will move the corresponding policy down one space in the table.

Note: The Outbound Policy works in a Top-Down fashion according to the Outbound Policy Table. This means that the firewall will apply the policies in order from the top of the table to the bottom. It is critical for both security and user accessibility to the WAN to have outbound policies in the correct order. See Section 1.9.1 for an example of this.

Edit: Clicking this button will display a table similar to the add table (see next page) to the bottom of the policy table that will allow you to modify the corresponding policy.

Delete: This will delete the corresponding policy.

Add Inbound Policy: Clicking on this button will bring up a table with all the add configurations as shown below:

Src IP: This specifies the Source IP for the Outbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu. The dropdown menu has four options:

- **Any IP**: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.

- **Single IP**: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

- **IP Range**: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.

• **Mask Range:** Selecting this will enable you to select a range of Subnet Masks to which the policy will apply. The first Subnet Mask in the range must be entered into the first IP Address entry field and the last Subnet Mask in the range must be entered into the second IP Address entry field.

Dest IP: This specifies the Destination IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and subnet mask(s) that will be affected by the policy. See **Src IP** above for configuration detail.

Src Port: This specifies the Source Port for the Inbound Policy. This is the internal (LAN side, behind firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

• **Any Port:** Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

• **Single Port:** Selecting this will cause only one Port to be affected by the policy. This Port will need to be specified by the user in the first Port entry field.

• **Port Range:** Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

• **Safe Ports:** Any port greater than 1024 (1025 – 65535) is considered a safe port.

Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (WAN side, outside of the firewall) Port that will be affected by the policy. See **Src Port** above for configuration detail.

Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

Filtering Action: This specifies what action the policy takes:

• **Allow:** Selecting this will cause the policy to allow packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

• **Deny:** Selecting this will cause the policy to deny packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

Time Window Filtering: This field allows you to select a certain time frame from the

Time Group in which this policy will be active. See section 6.6 for more information on Time Groups.

DB: Short for Database, this field allows you to select a user-defined IP Group for the

Src IP and **Dest IP** fields and a user-defined Service Group for the **Dest Port**. Userdefined IP and Service Groups are created in **IP Group** and **Service Group** pages.

1.9 Inbound/Outbound Policy Sample Configuration

This is a sample Inbound/Outbound configuration meant to guide you in making your own configurations. This configuration does not necessarily provide proper security, it is meant only as a sample to display the functionality of the Inbound and Outbound Policies.

1.9.1 Inbound Policy

Sample Configuration: You want your firewall to have the following properties:

- Accept all http IP addresses, except for 204.35.82.1

- Grant FTP access from 101.64.35.4 (external) to 10.0.0.3, 10.0.0.4, 10.0.0.5, and 10.0.0.6 (all internal).

- Deny all access to FTP Server 10.0.0.6 on the weekend. Converting the access requirements from above so that the Inbound Policy can understand them yields the following:

- Deny access from any Src (WAN) IP to any Des (LAN) IP through any source or destination port and through all protocols.

- Allow access from any Src (WAN) IP to any Des (LAN) IP through port 80 (HTTP), through TCP.

- Deny access from Src (WAN) IP 204.35.82.1 to any Des (LAN) IP through port 80 (HTTP), through TCP.

- Allow access from Src (WAN) IP 101.64.35.4 to Des (LAN) IP 10.0.0.3 ~ 10.0.0.6 through port 20 (FTP), through TCP.

- Deny access from any Src (WAN) IP to **DB** FTP (defined as) IP through any source or destination protocol and through all protocols during time period WEEKEND, where WEEKEND is defined in the **Time Group** as Saturday, 12:00AM to Sunday, 11:59PM.

It does not matter which order you input these in as long as you sort them into the correct order once you are finished.

Note: It should be clear now how critical it is to sort the policies in the correct order. For example, if policies one and two were switched, there would be NO HTTP access to any computer in the LAN. This would make web browsing impossible.

1.9.2 Outbound Policy

Sample Configuration: You want to deny all access to the WAN except for the following:

- HTTP access from any IP through TCP.

- Any access from 10.0.0.3 through any protocol.

- FTP Access from 10.0.0.3~10.0.0.6 through any protocol Converting the access requirements from above so that the Outbound Policy can understand them yields the following:

- Deny all access from any Src (LAN) IP to any Des (WAN) IP through any source or destination port and through any protocol.

- Allow access from Src (LAN) IP 10.0.0.3 to any Des (WAN) IP through any port through any protocol.

- Allow access from any Src (LAN) IP to any Des (WAN) IP through port 80 (HTTP), through TCP.

- Allow access from Src (LAN) IP range 10.0.0.3~10.0.0.6 to any Des (WAN) IP through port 20 (FTP), through any protocol.