CHAPTER 8

IntraGuard Firewall Configuration

There are three pre-set paths in the IntraGuard Firewall. A path defines a route for packets through the firewall. Each of the three paths already has a name, a security policy and interface definitions. While the names and parameters of the firewall paths can be modified, the default settings should work for many installations.

Firewall paths can be added to the edit area of a device, renamed or deleted.

To **Add** a path, right-click on any configuration item for the device, then select Firewall Path/Add Firewall Path from the popup menu.

The IntraGuard Firewall currently supports up to three firewall paths. Any additional paths may cause configuration problems. It is recommended that you add firewall paths only if you have previously deleted a path, so that no more than three paths exist at a time.

To **Rename** a path, right-click on the path's icon, then choose Firewall Path/Rename Firewall Path.

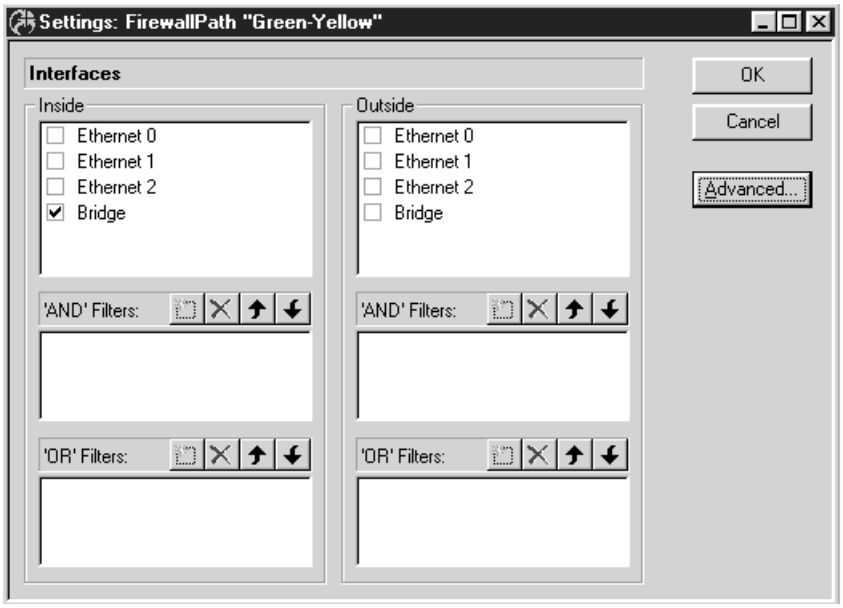
To **Delete** a path, right-click on the path's icon, then choose Firewall Path/Delete Firewall Path.

These functions are also available in the **File** menu.

Settings: FirewallPath Dialog Box

To access this dialog box (Figure 8-1), select FirewallPath/Settings from the Device View.

Figure 8-1 Settings: FirewallPath Dialog Box



Interfaces - Inside/Outside

These checkboxes control which interfaces will be specified as inside interfaces or outside interfaces for each path. Typically, **Inside** interfaces are secure while **Outside** interfaces are less secure.

If more than one interface is designated as an inside or outside interface on a particular path, those interfaces are considered to be open multiplexed and traffic will flow freely between them. For example, in the default configuration, both Ethernet 0 and the Bridge interface are inside interfaces on the Green-Red Path. Traffic between those two interfaces will not be subjected to firewall screening.

AND Filters

AND filters allow the device to accomplish packet filtering on packets that will be forwarded out the specified interface(s). AND filters are typically used to deny certain packets, so they are checked only for those protocols or ports which have been permitted by a Security Policy protocol setting, an Allow Ports/Protocol setting or an OR filter. Any packet not explicitly allowed by the rule set is dropped. Filters are created using the IP Filter Editor, described in the IP Filtering section of this manual. Up to four filter sets may be listed. The filters will be applied in the order listed.

Use the **New** button to add a named filter to the list or to select a named filter from a pull-down list.

Use the **Delete** button to remove a named filter from the list.

Use the **Move Up** and **Move Down** buttons to move the filters into the desired application order.

OR Filters

OR Filters allow the device to accomplish packet filtering on packets that will be forwarded out the specified interface(s). OR filters are typically used to permit certain packets, so they are checked only for those protocols or ports which have been denied by a Security Policy protocol setting or an Allow

Ports/Protocol setting. Any packet not explicitly allowed by the rule set is dropped. Up to four filter sets may be listed. The filters will be applied in the order listed. Filters are created using the IP Filter Editor, described in the IP Filtering section of this manual.

Use the **New** button to add a named filter to the list or to select a named filter from a pull-down list.

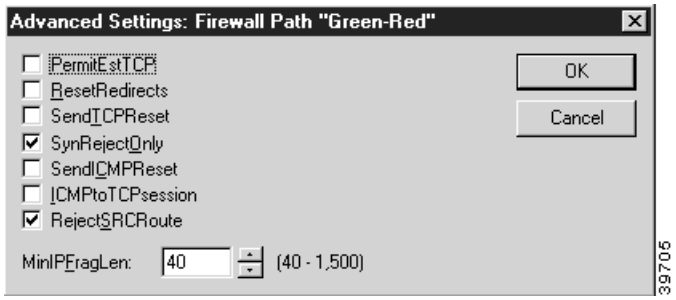
Use the **Delete** button to remove a named filter from the list.

Use the **Move Up** and **Move Down** buttons to move the filters into the desired application order.

Advanced Settings: Firewall Path Dialog Box

To access this dialog box (Figure 8-2), select FirewallPath/Settings from the Device View, then click on the **Advanced** button.

Figure 8-2 Advanced Settings: Firewall Path Dialog Box



These settings allow detailed control of how certain packet types and sessions will be handled on the path.

PermitEstTCP

This checkbox sets whether the path will permit TCP sessions for which the IntraGuard did not see the SYN flag. The SYN flag is included in the header of the first couple of TCP packets and indicates that a session is being established. When **checked**, this allows established connections to continue after rebooting the device, but it is also a less secure option. The default is unchecked.

ResetRedirects

This checkbox sets whether the device will terminate sessions on a firewall path where ICMP redirects have been sent. ICMP redirects are generated when a device cannot route a packet correctly on its own. The effect can be that three firewall path sessions will be created to route the packet correctly, two of which will not be needed after the first packet gets delivered. The default is unchecked.

SendTCPReset

This checkbox sets whether the device will send a TCP reset message to the client when a TCP session has been rejected. The default is unchecked.

SynRejectOnly

This checkbox sets whether the device will limit itself to sending TCP reset messages only when a TCP packet containing the SYN flag has been rejected. This can be useful when ICMP redirects are being sent, which could cause sessions to terminate prematurely. The default is checked.

SendICMPReset

This checkbox sets whether the device will send an ICMP message to the client when an IP or UDP packet has been rejected. The default is unchecked.

ICMPtoTCPsession

This checkbox sets whether the device will send an ICMP message to the client when a TCP packet has been rejected. This is in addition to sending a TCP reset message, if it has been enabled using the SendTCPReset checkbox. The default is unchecked.

RejectSRCRoute

This checkbox sets whether the device will reject source-routed IP packets. The default is checked.

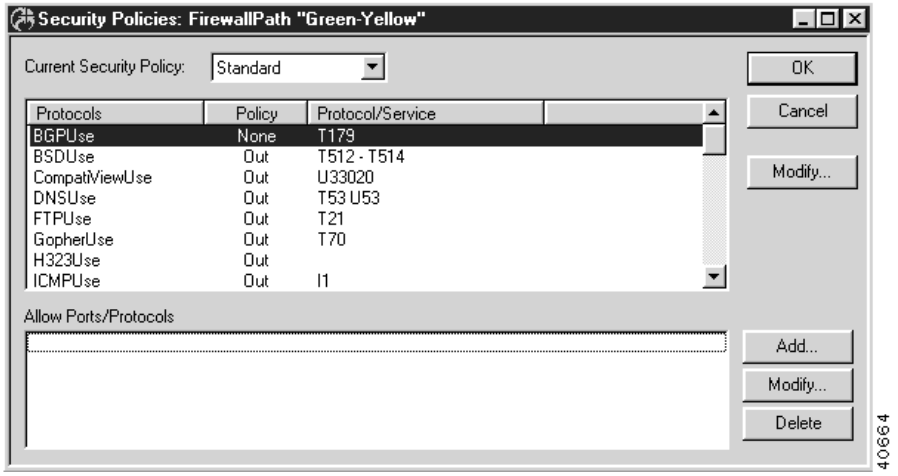
MinIPFragLen

This field sets the minimum acceptable length of IP packets. Raising the minimum packet length can be useful in preventing "frag" attacks, which can take advantage of the use of partial header information in fragmented packets. The IntraGuard protects against overlapping fragmentation attacks, even when the MinIPFragLen is set to the minimum value of 40. Values may range between 40 and 1,500. The default is 40.

Security Policies: Firewall Path Dialog Box

This dialog box (Figure 8-3) can be accessed by selecting FirewallPath/Security Policies from the Device View. This dialog box displays the overall security policy for an IntraGuard Firewall path and the individual policy settings for each protocol. It can be used to change the overall security policy, but not the individual protocol policy settings. To change individual protocol settings, see the Security Policy Protocol Setting dialog box.

Figure 8-3 Security Policies: Firewall Path Dialog Box



Current Security Policy

This pull-down menu sets the overall Security Policy for the path. There are five general policy sets, each of which has an associated list of protocol settings which define how the interfaces belonging to the path will handle those types of packets.

Definitions of the five sets of security policies follow:

- **Blocked** is the most secure policy set, which does not allow packets in or out along the path.
- **Strict** is a restrictive policy set. A small set of outgoing client sessions are permitted through the firewall and all incoming sessions are excluded.
- **Standard** is a moderately restrictive policy set. Almost all outgoing client sessions are permitted and almost all incoming server sessions are excluded. The only exceptions to those rules are that the BPG and X Window protocols are excluded from going in or out along the path.
- **Lenient** is a less secure policy set. All outgoing client sessions are permitted and some incoming server sessions are permitted.
- **Open** is an insecure policy set. Everything is permitted through the firewall, thereby turning the firewall into a transparent bridge.

Changing the Current Security Policy will override any individually made protocol settings.

Security Policies at a Glance

The following chart shows how each of the 31 protocols is treated by each of the five sets of security policies. The protocol BGPUse, for example, is assigned the security policy None by the Blocked policy set, but it is assigned the security policy Both by the Open policy set.

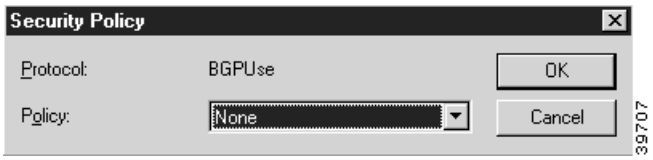
Protocol	Security Policy				
	Blocked	**Strict**	**Standard**	**Lenient**	**Open**
BGPUse	None	None	None	Both	Both
BSDUse	None	None	Out	Out	Both
CompatiViewUse	None	Out	Out	Both	Both

DNSUse	None	Out	Out	Both	Both
FTPUse	None	Out	Out	Both	Both
H323Use	None	None	Out	Out	Both
ICMPUse	None	None	Out	Out	Both
IPsecUse	None	Out	Out	Both	Both
IRCUse	None	None	Out	Out	Both
LPRUse	None	None	Out	Out	Both
MailUse	None	Out	Out	Both	Both
NFSUse	None	None	Out	Out	Both
NetBIOSUse	None	None	Out	Out	Both
NewsUse	None	None	Out	Out	Both
NonIPUse	None	None	Out	Out	Both
OSPFUse	None	None	Out	Out	Both
POPUse	None	None	Out	Out	Both
RIPUse	None	None	Out	Out	Both
RealAudioUse	None	None	Out	Out	Both
SunRPCUse	None	None	Out	Out	Both
TelnetUse	None	Out	Out	Out	Both
TFTPUse	None	Out	Out	Out	Both
TunnelUse	None	None	Out	Out	Both
WebUse	None	Out	Out	Both	Both
XWinUse	None	None	None	In	Both
ISAKMPUse	None	Out	Out	Both	Both
GopherUse	None	Out	Out	Out	Both
NTPUse	None	None	Out	Both	Both
OtherTCPUse	None	None	Out	Out	Both
OtherUDPUse	None	None	Out	Both	Both
OtherUse	None	None	Out	Both	Both

Security Policy Protocol Setting Dialog Box

To change the individual protocol settings, select a protocol in the Security Policies: Firewall Path dialog box (Figure 8-4) and click the **Modify...** button. The Security Policy dialog box will appear in the Main Window.

Figure 8-4 Security Policy Protocol Setting Dialog Box



Changing the Current Security Policy will override any individually made protocol settings.

Policy

This pull-down menu allows you to set how the selected protocol's packets will be handled on the path.

- **In** means that a protocol will be allowed through to the inside interface(s) of a path.

- **Out** means that a protocol will be allowed through to the outside interface(s) of a path.
- **None** means that a protocol will be allowed neither in nor out.
- **Both** means that a protocol will be allowed both in and out.

Protocols

- **BGPUse** defines how BGP (Border Gateway Protocol) packets will be handled on the path. BGP is the routing protocol between Internet backbone routers.
- **BSDUse** defines how BSD packets will be handled on the path. BSD is the UC Berkeley remote execution and terminal session protocol. RSH, RCP, RLogin, and RExec are the protocols supported.
- **CompatiViewUse** defines how the Cisco VPN 5000 Manager packets will be handled on the path. This is Cisco's VPN 5000 GUI manager. This option also defines handling for earlier versions of STAMP, an older tunnel authentication protocol.
- **DNSUse** defines how DNS (Domain Name Service) packets will be handled on the path. DNS is the protocol which translates IP addresses into hostnames and hostnames into IP addresses.
- **FTPUse** defines how FTP (File Transfer Protocol) packets will be handled on the path. Dynamic sessions are created for file transfers using the PASV and PORT commands.
- **H323Use** defines how H323 packets will be handled on the path. H323 is a video and audio conferencing protocol.
- **IPsecUse** defines how IPsec (Internet Protocol Security) packets will be handled on the path. Both encrypted (ESP) and authenticated (AH) packets are supported.
- **IRCUse** defines how IRC (Internet Relay Chat Protocol) packets will be handled on the path.
- **LPRUse** defines how LPR packets will be handled on the path. LPR is a network printing protocol.
- **MailUse** defines how SMTP (Simple Mail Transfer Protocol) packets will be handled on the path. This protocol is used to send mail between servers.
- **NFSUse** defines how NFS (Network File Sharing Protocol) packets will be handled on the path. To permit NFS In, it may be necessary to set SunRPCUse to In as well.
- **NetBIOSUse** defines how NetBIOS packets will be handled on the path. NetBIOS is Microsoft's file sharing protocol.
- **NewsUse** defines how NNTP (Network News Transfer Protocol) packets will be handled on the path.
- **NonIPUse** defines how non-IP packets will be handled on the path. This would include other protocols such as AppleTalk and IPX.
- **OSPFUse** defines how OSPF (Open Shortest Path First) packets will be handled on the path. OSPF is a link state routing protocol.
- **POPUse** defines how POP packets will be handled on the path. POP is a mail client protocol. This protocol allows users to receive mail.
- **RIPUse** defines how RIP (Routing Information Protocol) packets will be handled on the path.
- **RealAudioUse** defines how Internet Real Audio Protocol packets will be handled on the path. Real Audio is an audio and video conferencing protocol.

- **SunRPCUse** defines how SunRPC (Sun's Remote Procedure Call Protocol) packets will be handled on the path. The SunRPC Protocol is used by NFS and other UNIX utilities to get the server's port address.
- **TelnetUse** defines how Telnet packets will be handled on the path. Telnet is a virtual terminal protocol.
- **TFTPUse** defines how TFTP (Trivial File Transfer Protocol) packets will be handled on the path.
- **TunnelUse** defines how GRE (General Router Encapsulation) packets will be handled on the path. GRE packets are IP-encapsulated tunneled packets. This option does not work with non-STEP tunnels (e.g. STAMP tunnels), which are enabled using the CompatiViewUse protocol.
- **WebUse** defines how HTTP (Hypertext Transfer Protocol) packets will be handled on the path. HTTP is the World Wide Web protocol. This option affects only HTTP packets; Telnet and FTP must be enabled individually to allow users to reach FTP sites or Telnet via the web. See the TelnetUse and FTPUse protocols.
- **XWinUse** defines how X Windows packets will be handled on the path. X Windows is the UNIX GUI.
- **GopherUse** defines how Gopher packets will be handled on the path. Gopher is a file transfer and browsing protocol.
- **ISAKMPUse** defines how ISAKMP (Internet Security Association Key Management Protocol) packets will be handled on the path. ISAKMP is the VPN (Virtual Private Network) key management protocol used by Cisco's VPN 5000 products.
- **NTPUse** defines how NTP (Network Time Protocol) packets will be handled on the path.
- **OtherTCPUse** defines how all other TCP-based protocols will be handled on the path.
- **OtherUDPUse** defines how all other UDP-based protocols will be handled on the path.
- **OtherUse** defines how IP packets which are not included in the other pushbutton options will be handled on the path.

Allow Ports/Protocols Dialog Box

To access the Allow Ports/Protocols dialog box (Figure 8-5), select the **Add...** button to the right of the Allow Ports/Protocols list in the Security Policies: Firewall Path dialog box.

Figure 8-5 Security Policy Protocol Setting Dialog Box

This dialog box allows you to specify a handling method for any numbered port or named protocol which isn't already an explicit Security Policy option. All Security Policy protocol settings take precedence over the Allow Ports/Protocols options. For example, if the **OtherTCPUse** option is set to In in the Security Policy settings, then it would be unnecessary to specify any particular TCP port using the **TCPInPort** option.

Port/Protocol

- The **TCPInPort** option specifies that a TCP port number will be allowed in along the path.
- The **TCPOutPort** option specifies that a TCP port number will be allowed out along the path.
- The **UDPInPort** option specifies that a UDP port number will be allowed in along the path.
- The **UDPOutPort** option specifies that a UDP port number will be allowed out along the path.
- The **IPInProto** option specifies that an IP protocol will be allowed in along the path.
- The **IPOutProto** option specifies that an IP protocol will be allowed out along the path.

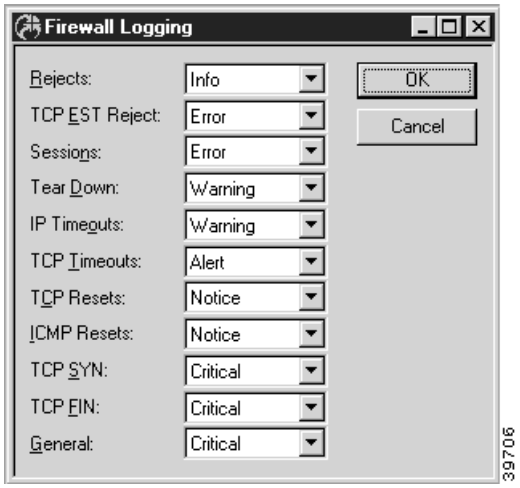
Port/Protocol Number

The port or protocol number must be specified as a decimal number between 0 and 65,535. RFC 1700 "Assigned Numbers" contains a listing of all currently assigned IP protocol numbers.

Firewall Logging Dialog Box

To access this dialog box (Figure 8-6), select Global/Firewall Logging from the Device View.

Figure 8-6 Firewall Logging Dialog Box



The logging settings define the level at which specific events are logged. The nine logging levels are listed in descending order of importance.

- Off
- Emergency
- Alert
- Critical
- Error
- Warning

- Notice
- Info
- Debug

The IntraGuard "tags" the log messages associated with each type of event with the specified log level. The **Off** setting will disable log messages for the event.

The event log messages will appear in the log buffer (or wherever log messages are being sent), only if the global log level is at the same level or a lower level of importance. This allows you to closely monitor certain events while excluding events you do not wish to closely monitor from the log.

Logging parameters for the device, including the global log level, are set in the Logging Configuration dialog box, which can be accessed by selecting Logging from the Device View.

Using the default configuration as an example, if you wish to see log messages for TCP Resets, which have a default setting of Notice, you would need to set the **Log Level** in the Logging Configuration dialog box to Notice, Info or Debug. Any other setting would mean that TCP Resets would not appear in the log.

Rejects

Rejects messages are created by the firewall whenever an IP packet is rejected for any reason. The default is Info.

TCP EST Reject

TCP EST Reject messages are created by the firewall whenever an established TCP session is rejected. These messages are also created when a TCP session for which the firewall has not seen the SYN flag is established. The default is Error.

Sessions

Sessions messages are created by the firewall whenever an IP session is established. The default is Error.

TearDown

TearDown messages are created by the firewall whenever an IP session is torn down. The default is Warning.

IP Timeouts

IP Timeouts messages are created by the firewall whenever a non-TCP session (i.e. IP or UDP session) is timed out. The default is Warning.

TCP Timeouts

TCP Timeouts messages are created by the firewall whenever a TCP session is timed out due to inactivity. The default is Alert.

TCP Resets

TCP Resets messages are created by the firewall whenever a TCP session is reset. The default is Notice.

ICMP Resets

ICMP Resets messages are created by the firewall whenever a non-TCP session (i.e. UDP or ICMP session) is reset. The default is Notice.

TCP SYN

TCP SYN messages are created by the firewall whenever a TCP connection cannot be completed because it was timed out. The default is Critical.

TCP FIN

TCP FIN messages are created by the firewall whenever a TCP connection cannot be properly torn down and is instead timed out. The default is Critical.

Redirects

Redirects messages are created by devices on the network when they receive a misdirected packet. These messages sometimes indicate route instability or the presence of an incorrectly configured IP host, but they do not necessarily indicate a problem on the network. The default is Critical.

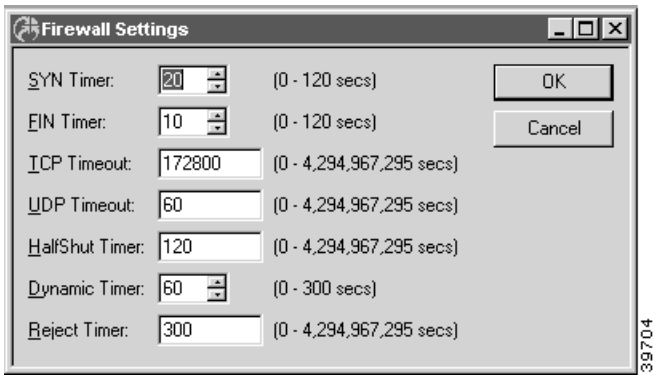
General

General messages are created when errors occur within the IntraGuard. This might include running out of memory or internal state errors, and should be infrequent. The default is Critical.

Firewall Settings Dialog Box

To access this dialog box (Figure 8-7), select Global/Firewall Settings from the Device View. The dialog box Firewall Settings appears on the Main Screen.

Figure 8-7 Firewall Settings Dialog Box



This dialog box is used to set global timers for the firewall.

SYN Timer

This field sets the number of seconds the firewall will wait without receiving a response to a SYN TCP packet before clearing a TCP session. The SYN flag is included in the header of the first couple of TCP packets and indicate that a session is being established. If the SYN Timer is set too low, half-open sessions may accumulate. If the SYN Timer is set too high, there may not be enough time to complete the handshake and establish a session. Values may range from 0 to 120. The default is 20 seconds.

FIN Timer

This field sets the number of seconds the firewall will wait without receiving a response to a FIN TCP packet before clearing a TCP session. TCP specifies that for a session to be fully closed down, both ends of the connection must send out a FIN packet. If the FIN Timer is too high, half-shut sessions may accumulate. If the FIN Timer is too low, sessions may be shut down too quickly. Values may range from 0 to 120. The default is 10 seconds.

TCP Timeout

This field sets the number of seconds the firewall will wait before shutting down an inactive TCP session. Values may range from 0 to 0xFFFFFFFF. The default is 172,800 seconds (48 hours).

UDP Timeout

This field sets the number of seconds the firewall will wait before shutting down an inactive non-TCP session. Values may range from 0 to 0xFFFFFFFF. The default is 60 seconds.

HalfShut Timer

This field sets the number of seconds the firewall will wait to close down a half-shut, inactive TCP session. TCP specifies that for a session to be fully closed down, both ends of the connection must send out a FIN packet. If the firewall has not received a FIN packet from the other end and there has been no activity during the specified length of time, the firewall will clear the session. Values may range from 0 to 0xFFFFFFFF. The default is 120 seconds. Setting a value of 0 will disable the timer.

Dynamic Timer

This field sets the number of seconds the firewall will wait before shutting down an inactive dynamic session. Dynamic sessions are created by the firewall to allow TCP sessions or non-TCP packets to come through the firewall. The firewall does this by monitoring packet headers and data, and then opening permitted sessions only when necessary. Values may range from 0 to 300. The default is 60 seconds.

Reject Timer

This field sets the number of seconds the firewall will keep track of rejected packets after the packet flow has ended. The firewall tallies the different types of rejected packets and summarizes the information in a display using the **show firewall rejects** command (see **firewall(show)** in the ***Cisco VPN 5000 Concentrator Series Command Reference Guide***). Values may range from 0 to 0xFFFFFFFF. The default is 300 seconds. If the Reject Timer is set to 0, the firewall will log every rejected packet individually, without summarizing them in a tally.