GNAT Box®

SYSTEM SOFTWARE

VERSION 3.4

User's Guide

ADDENDUM

Global
Technology
Associates, Inc.

Copyright

GNAT Box System Software User's Guide version 3.4 Addendum **July 2003**

Technical Support

GTA includes 30 days installation support from the day you receive the initial shipment. GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local GTA authorized channel partner.
Tel: +1.407.482.6925 Email: support@gta.com

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks

GNAT Box is a registered trademark of Global Technology Associates, Incorporated. RoBoX and Surf Sentinel are trademarks of Global Technology Associates, Incorporated.

GTA acknowledges all trademarks appearing in this document. This product includes software developed by the University of California, Berkeley and its contributors. Netscape Navigator is a trademark of Netscape Communications Corporation. Internet Explorer is a trademark of Microsoft Corporation. Cerberian is a trademark of Cerberian, Inc. CyberNOT and SurfControl are trademarks of SurfControl, plc, and may be registered in certain jurisdictions. MAPS is a service mark of Mail Abuse Prevention System, LLC. WELF and WebTrends are trademarks of NetIQ. All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA
Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: http://www.gta.com • Email: info@gta.com
Lead Development Team: Larry Baird, Richard Briley, Jim Silas, Brad Plank.
Technical Consulting: David Brooks. **Documentation:** Mary Swanson.

Contents

1 Introduction

Overview

GNAT Box System Software version 3.4 offers more versatility with enhancements to PPP, logging, filters and tunnels, updates for cross-platform utilities, and new options for content filtering. These features include:

- **PPTP support**
- **Enhanced PPP for high-speed DSL**
- **Ability to record "To" and "From" addresses using email proxy**
- **Additional logging and filter options**
- **User authentication for tunnels and filters**
- **New fields and layout for inbound tunnel configuration**
- **Updated Surf Sentinel and Surf Sentinel Plus**
- **User-defined blocking message for content filtering**
- **Browser-based Help for the Web Interface**
- **New and enhanced GTA utilities:**
  DBmanager, GTAsyslog, LogView and GBAuth

About this Addendum

This addendum is a supplement to the **GNAT Box System Software User's Guide version 3.3** and includes a description of the major changes that have been introduced since the version 3.3 manual.

Additional Documentation

For instructions on installation, registration and setup of a GTA Firewall in default configuration, see your GTA Firewall's product guide; for optional features, see the appropriate Feature Guide. User's Guides, Product Guides and Feature Guides are delivered with new GTA products; these manuals and other documentation for registered products can also be found on the GTA website, www.gta.com.

Documents on the website are either in plain text (*.txt) or Portable Document Format (PDF; *.pdf) which requires Adobe Acrobat Reader version 5.0. A free copy of the reader can be obtained at www.adobe.com. Documents received from GTA Support may also be in email or Microsoft Word format (*.doc).

Documentation Map

Products and Options

GNAT Box System Software	GNAT Box System Software User's Guide
GTA Firewall Installation	Product Guides
Global Management System for Firewalls	GMS User's Guide
Reporting	GTA Reporting Suite User's Guide
Content Filtering	Surf Sentinel Content Filtering Feature Guide
High Availability	H_2A High Availability Feature Guide
Virtual Private Networking	GNAT Box VPN Feature Guide
VPN Examples	GNAT Box VPN to VPN Tech Docs

Utilities & Information

Logging Utilities	GNAT Box System Software User's Guide & Addendum
Database Maintenance	GMS & GTA Reporting Suite User's Guides
Troubleshooting	Product and Feature Guides
Ports & Services	Product CDs
Drivers & NICs (GNAT Box Pro, Flash)	www.gta.com
Frequently Asked Questions	FAQs on www.gta.com
Web Interface, GBAdmin	GNAT Box System Software User's Guide
Console interface	Console Interface User's Guide

2 Basic Configuration

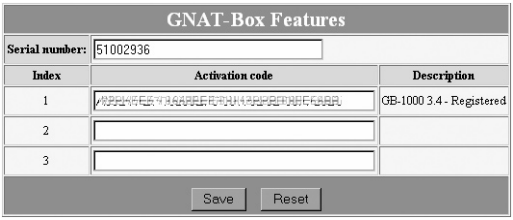
Additions and changes to the functions in Basic Configuration include:

- **Support for PPTP**
- **Product serial number entry moved to the Features screen**

Features

Use the Features screen to enter GTA Firewall activation codes for options such as H_2A, Surf Sentinel and GNAT Box VPN. System activation codes will also appear.

The serial number field, previously in the Preferences/Contact Information screen, is now located in Features. This change reflects the order in which GNAT Box System Software is configured: serial number, then features. Preferences still contains administrator contact information, the product support email address and the default character set selection field.



GNAT-Box Features

Serial number:	51002936	
Index	**Activation code**	**Description**
1	[illegible]	GB-1000 3.4 - Registered
2		
3		

Save Reset

Features

PPP

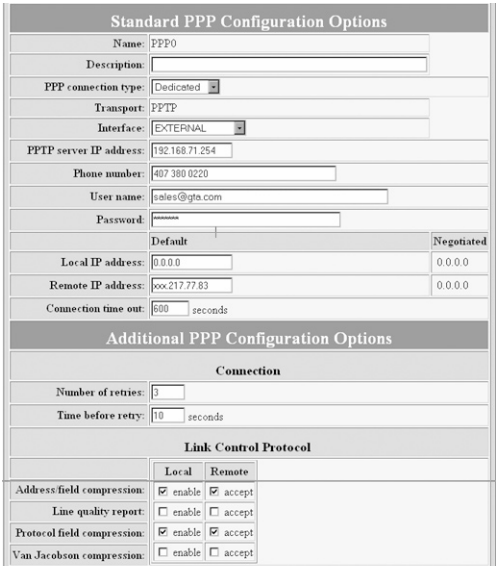
Configure a PPP (Point-to-Point Protocol) connection for the firewall in the PPP section. The fields in each section will vary depending on whether standard PPP, PPPoE or PPTP is selected.

PPTP

PPTP (Point-to-Point Transport Protocol) is a specialized PPP (point-to-point) transport protocol for some Microsoft products. A PPTP connection on GNAT Box System Software allows a link from a non-routable internal IP address to an external IP address through the use of an internal PPTP server with a routable IP address. The PPTP configuration fields vary from standard PPP. Use the fields below to create a PPTP connection.

To configure a PPTP connection, open the PPP section and add an entry. In the transport dialog box, select PPTP transport.

PPTP Fields	
Name	PPP connections are automatically named PPP0, 1, 2, 3 or 4, in order of creation. When an entry is deleted, the remaining entries are renamed in the new list order. Interfaces referencing PPP must be changed to match.
Description	Define a name for the connection.
Connection Type	Select Dedicated. Establishes a link when the firewall boots up. The link will remain up until the interface is manually disabled, or the system is halted.
Transport	PPTP (non-configurable in this screen).
Interface	Select the interface defined later in Network Information.
PPTP server	Enter IP address of the internal PPTP server.
Phone Number	Number used to dial the remote site, if required.
User Name Password	Enter the User ID and password for remote access.
Local & Remote IP address	If the remote site supports dynamic address assignment, leave the local address set to the default, 0.0.0.0, and set the remote IP to an address on the remote network, such as the router or the DNS server. PPP will use that address to negotiate the actual value. If the Remote IP address is static (dedicated), enter the address and leave the Local IP address set to 0.0.0.0. If both addresses are static, enter an address for both fields.
Connection time out	Time a connection will stay connected when inactive. Default is 600 seconds. Enter "0" to prevent timing out.
Link Control Protocol	
Address/field compression	Enable and Accept selected by default.
Line quality report	Deselected by default.
Protocol field compression	Enable and Accept selected by default.
Van Jacobson compression	Deselected by default.



PPTP Screen

Select PPTP for External Interface

After configuring PPTP, go to Network Information to set up an External interface using the PPTP connection.

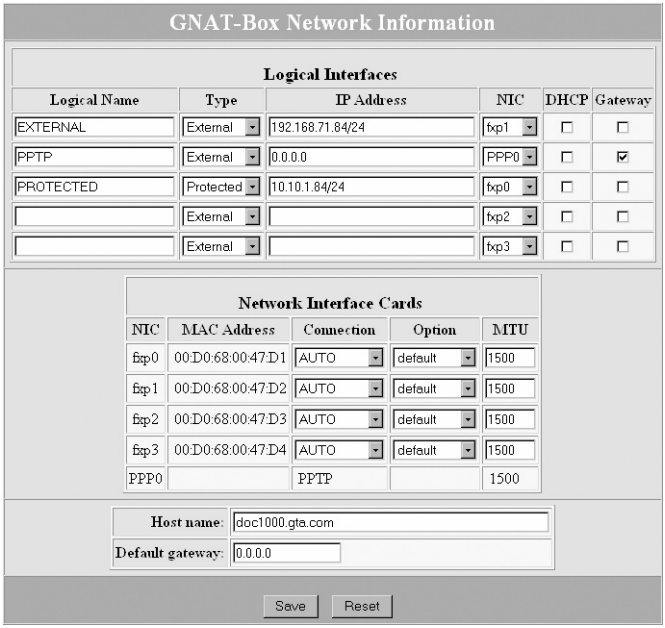
In the NAME field, enter a name for the connection. (This will name the Interface Object and also designate the physical connection.) In the TYPE field, select External, and in the next field, enter the IP address assigned to the PPTP connection. Select PPTP from the NIC (Network Interface) dropdown box. Finally, select the Gateway checkbox and save the section.

Caution

PPP connections are automatically named PPP0, 1, 2, 3 or 4, in order of creation. When an entry in the PPP section is deleted, the remaining entries will be renamed according to the new order. Interfaces which use PPP connections must be changed to the revised designations.

Enable the PPTP Connection

Open PPTP again. Select the Interface Object created in Network Information and save the section.



Network Information

Create a Remote Access Filter

A Remote Access Filter must be defined and enabled to allow GRE (Generic Routing Encapsulation) access to the PPTP server. Once you have completed the PPTP connection, auto-configure the Remote Access Filter set using the Default button, or manually add the filter below in which the Source is the IP address for the ISP and Destination is the PPTP server IP address. Auto-configured filters are broad in scope and may require modification to meet your security policy.

Once the settings have been saved, the PPTP connection will dynamically negotiate the gateway IP address.

Description:	Allow GRE from PPTP server.
Type:	Accept
Interface:	ANY
Authentication required:	Select
Protocol:	GRE (Protocol 47)
Source:	<Use IP address> e.g., 192.168.71.220
Source Port:	Blank
Destination:	<Use IP address> e.g., 10.0.0.81
Destination Port:	Blank

Fields not illustrated above can use the defaults or custom settings.

3 Services

Additions and changes to Services functions include:

- **Email Proxy records SMTP "To" and "From" fields**
- **Remote Logging screen updated**
- **GMS Server name change**

Email Proxy

The Email Proxy is used to configure an SMTP (Simple Mail Transfer Protocol) proxy for inbound email on TCP port 25. The administrator can use the Email Proxy to shield an internal email server from unauthorized access and reduce or eliminate unsolicited email (spam).

Caution

An inbound tunnel on TCP port 25 will bypass the Email Proxy for the IP address specified in the tunnel definition, therefore GTA recommends not creating an inbound tunnel on the same IP address and port as the Email Proxy.

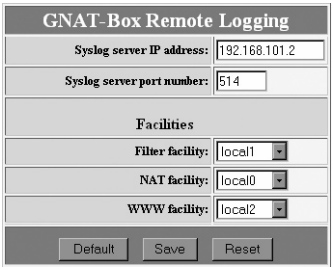
The Email Proxy compares the source IP address of incoming messages to the IP addresses of known spammers listed in the enabled Mail Abuse Prevention RBLs (Realtime Blackhole Lists). If a source matches one of these, the IP address is logged, and the message is permanently rejected (the firewall returns a "do not send again" packet to the source IP address) and dropped.

In GNAT Box System Software version 3.3.2, the Email Proxy added the ability to append the To and From addresses contained in the initial SMTP conversation to the log messages as X-To and X-From.

Remote Logging

Remote Logging provides a means to configure how and where log information is sent. GNAT Box System Software uses the syslog TCP/IP protocol for recording logs remotely. The Remote Logging screen has also been simplified to take advantage of the WELF logging now used on GTA Firewalls. See the Appendix for more information about new log options and messages.

Filter priority numbers are still used for individual filters. The logging for opening and closing tunnel connections (tunnel "opens" and "closes") is now selected in Filter Preferences.



Remote Logging

Remote Logging Fields

Syslog server IP address	The IP address of a host system that will accept the remote logging data. Remote logging data can be accepted by the supplied GTAsyslog logging facility or any program that accepts the syslog protocol.
Syslog server port number	Port used to connect with the GTAsyslog server IP address. This is port 514 by default.

Facilities

Unix syslog facilities: auth, authpriv, console, cron, daemon, ftp, kern, lpr, mail, news, ntp, security, user, uucp, and local0 - local7
Disable by selecting None from the list.

Filter Facility	Logs information associated with any filter that has logging enabled. Any attempts at unauthorized access will be logged to the Filter Facility log stream.
NAT Facility	Logs information associated with Network Address Translation: essentially, outbound packets.
WWW Facility	Logs all URLs accessed through the GTA Firewall.

4 Authorization

The Authorization section includes these added or changed functions:

- **GBAdmin user interface now uses SSL**
- **SSL certificate renewal moved to Remote Admin/Authentication**
- **SSL certificate now automatically renewed on upgrade**
- **User validation expanded**
- **Explanation of Security Association tracking for VPNs**

SSL Encryption

SSL encryption is selected by default in GNAT Box System Software installations after 3.3.2. SSL may be configured from either GBAdmin or the Web user interface. SSL requires a Remote Access Filter with a port matching the Remote Administration port (443, by default).

New SSL Certificate

The New SSL Certificate function is now a selection on the Remote Administration/Authentication screen. GNAT Box System Software version 3.4 adds the ability to use SSL encryption with the GBAdmin user interface. A New SSL Certificate can now be generated from GBAdmin.

SSL Certificate Renewal

Each time you upgrade GNAT Box System Software, the SSL certificate is renewed for a year from the release build date.

Remote Administration/Authentication

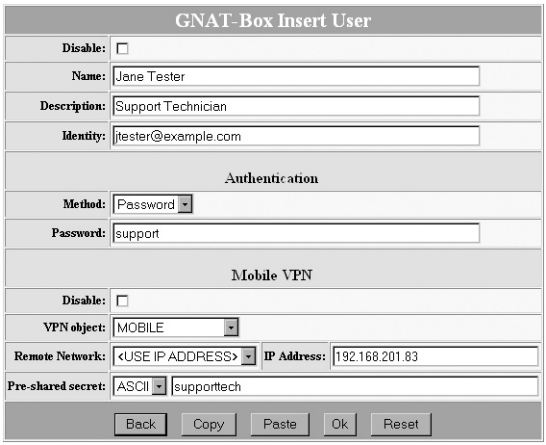
Users

The Users screen allows the administrator to create a user and indicate whether that user is enabled for general access, VPNs, or other restricted access points, expanding the use of user IDs from mobile authentication.

The Users section also allows the creation and authorization of GTA Firewall mobile VPNs using addresses or objects. One or more mobile VPNs are defined by linking a VPN object (such as the VPN object **MOBILE**) to a remote network address or address object. See the next section, VPNs, for more about GTA Firewall VPNs.

The remote network for mobile VPNs can now be indicated by selecting either an address object or entering an IP address.

Users can be selected in filters to regulate access from outside the Protected Network and in Inbound Tunnels to restrict access from a specified network interface to an IP address/port. See Chapter 6 – All Filters to learn more about User Authorization. See the Chapter 9 – Utilities for more about authentication using GBAuth.

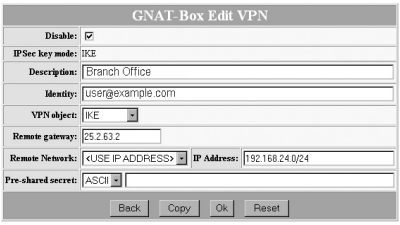


Users Authorization

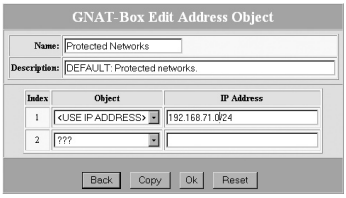
VPNs

The VPNs section allows the creation and authorization of GTA Firewall VPNs using addresses or objects. One or more VPNs are defined by linking a VPN object to a remote network address or address object.

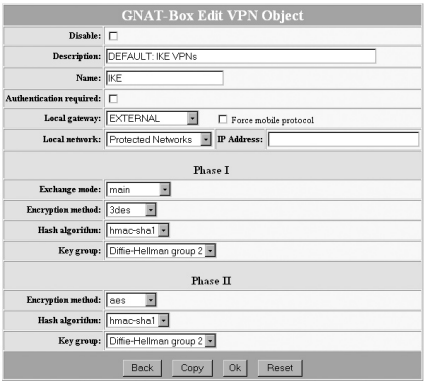
The authorization of a VPN connection between two single networks defines one VPN. For example, in the VPN authorization illustrated below, the local network VPN object **IKE** contains the address object **Protected Networks**, which in turn represents all the protected networks in the home office. The remote network is single network address. Any subnets have been combined to create one network using a /24 netmask.



VPN Authorization



Address Object



VPN Object

Security Associations

A Security Association (SA) specifies the parameters connecting two hosts. Each two-way connection uses a minimum of two SAs, one for each direction of communication. Any time a defined VPN is active (in use, or not yet timed out), it will use at least two SAs.

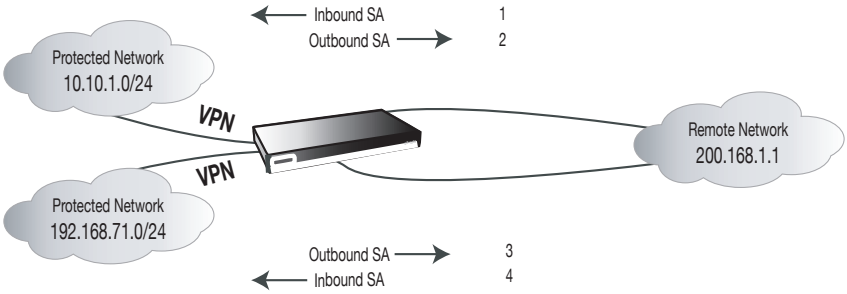
For the total number of potential SAs used by each VPN authorization, see the Authorization section in the system configuration report, found in **Reports > Configuration**. See product guides for the number of Security Associations supported by a specific GTA Firewall. To see the current number of VPN Security Associations, see **System Activity > Active VPNs**. Each active VPN will have two entries, one for each direction of communication.

Note

Each VPN authorization in the configuration report will contain one or more VPNs, depending on the number of networks represented by each VPN or address object.

Multiple Networks

A GTA Firewall VPN authorization can define one VPN or many, depending on the number of networks represented by each object. For example, if a VPN authorization contains an object with two separate local networks and a single remote network, two VPNs are defined, for a total of four SAs.



Two VPNs, four VPN Security Associations

Mobile Protocol

A VPN using mobile protocol – either a mobile VPN created in the **Authorization > Users** section, or gateway to gateway VPN with **Force Mobile Protocol** selected – will use SAs while active. The number of SAs potentially used by mobile and gateway to gateway VPNs can be higher than the number of licensed SAs; however, the number of SAs used by active VPNs, mobile VPNs included, cannot exceed this number. See the previous section for more about changes to Users authorization.

5 Content Filtering

Additions and changes to Content Filtering include:

- **Mobile Code Blocking moved to Access Control Lists**
- **Surf Sentinel Plus* updated to Cerberian Web Filter 2.0**
- **URL blocks now include user-defined message and/or web page for the Transparent Proxy**

* A GNAT Box System Software option.

Note

See the GNAT Box System Software User's Guide for instructions on how to use other content filtering options.

Access Control Lists

Access Control Lists (ACLs), one of GTA's Internet access management solutions, provide a means to select web access control facilities and specify how they will be applied to web requests. GTA Firewalls have three primary functions for access control: Access Control Lists (ACLs), Local Content Lists (LCLs) and proxy settings. In addition, records of blocked sites are created and sent to GTA Firewall logs.

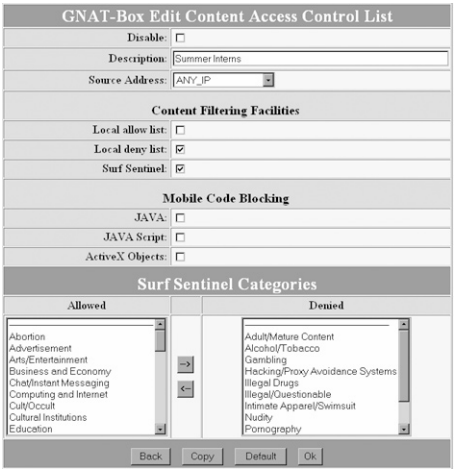
Mobile Code Blocking

Mobile Code Blocking for JAVA, JAVA Script and ActiveX objects is built in. These objects or scripts appear in inbound HTML on TCP port 443, 80, 8000 and 8080. Mobile Code Blocking has been moved from Content Filtering Preferences, where it was applied as a global option, to individual ACLs that allow the user to select mobile code blocking for groups defined in each ACL.

Access Control Lists (ACL) Fields

Disable	Select this checkbox to disable the designated ACL.
Description	Enter a description for the ACL.
Source Address	If a request matches an element of the specified address object, the packet will be compared to the ACL.
	Content Filtering Facilities*
Local Allow List	Select to process against GTA's Allow list.
Local Deny List	Select to process against GTA's Deny list.
Surf Sentinel	Select to process against the Surf Sentinel list.
	Mobile Code Blocking
JAVA	Disabled by default.
JAVA Script	Disabled by default.
ActiveX Objects	Disabled by default.
	Surf Sentinel Categories
	Allow or block URLs in Surf Sentinel categories. Switch a category from one list to the other by selecting the item and clicking the left or right arrow button.

* CyberNOT fields will display for those with a current CyberNOT feature code.



Access Control Lists

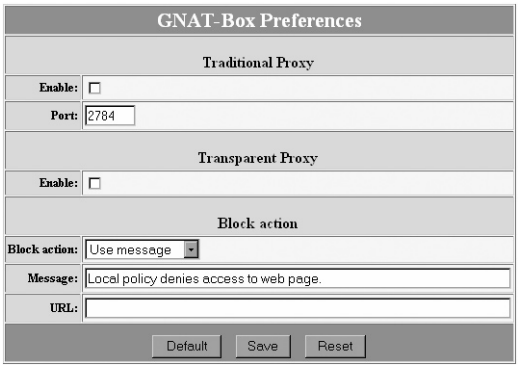
Content Filtering Preferences

Content filtering requires the use of an HTTP proxy. Preferences allows the administrator to specify the use of the Traditional Proxy and associated port, the Transparent Proxy, or both; in addition, a customizable block action (a message or URL) can be selected.

If an ACL blocks a web address (URL), and a user attempts to load a page from that address, the user will see a message, or be redirected to a URL, e.g., an internal website that defines the company's Internet use policies and the administrative process to get access to a site. The default message, "Local policy denies access to web page," will appear if a user attempts to reach a blocked address unless a custom message is entered.

Content Filtering Preferences Fields

	Traditional Proxy
Enable	Select this checkbox to enable the traditional proxy.
Proxy Port	Port through which the proxy will run. Default is 2784.
	Transparent Proxy
Enable	Select this checkbox to enable the transparent proxy.
	Block Action
Block Action	Select "Use message" or "Redirect to URL."
Message	If message is selected, enter a custom message or use the default, "Local Policy denies access to web page."
URL	If URL is selected, enter the address of the web page to which blocked users will be redirected. If the web site is encrypted, (port 443) use `https://address`. If the site is unencrypted (port 80 or 8080), use `http://address`.



Content Filtering Preferences

6 All Filters

Filters control access to and through the GTA Firewall. Functions for creating Outbound and Remote Access Filters are under the Filters section, while the functions for creating IP Pass Through Filters is in the IP Pass Through section. Outbound, Remote Access and IP Pass Through use the same mechanisms for filter configuration, so the changes noted refer to all filters.

The following features have been added or changed in the filters sections:

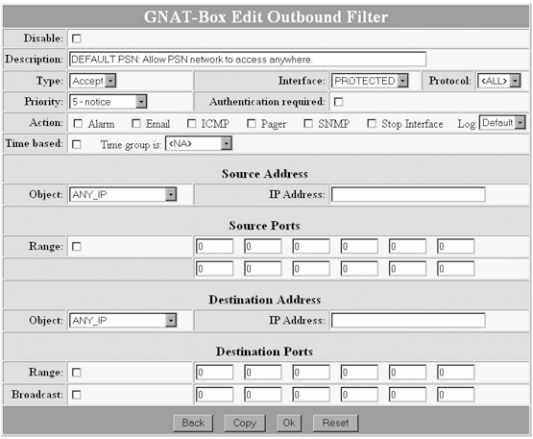
- **Automatic Filters are logged by the system and can be disabled.**
- **User names on email rejected by SMTP proxy can be logged.**
- **Users authenticated by GBAuth can be logged.**
- **Authentication can be selected for any filter definition.**
- **Users, received packets and sent packets for tunnels can be logged.**
- **ICMP packets dropped by Stealth mode can be logged.**
- **Default logging selection is simplified, and tunnel connection opening events can be logged.**

Filter Definition

Users created in User Authentication can now be required to enter a user name and password when accessing the firewall using a filter or an inbound tunnel.

New and streamlined logging options have changed the defaults for the Log field's **Default** setting. See Filter Preferences for more about default logging.

The **Yes** setting logs all events associated with the filter, including tunnel connections ("opens" and "closes"), filter blocks, accepts. The administrator can use these logs to examine filter effectiveness and test configurations without setting the option globally.



Filter Definition

Filter Fields

Description	Enter a description of the filter for reference. Filters generated by the system will have default descriptions.
Disable	Check to disable the selected filter.
Type	Accept or Deny the packet type.
Interface	Choose the physical interface this filter will affect by selecting its name. The specified physical interface is matched against the interface on which the IP packet arrived. <ANY> will match any physical interface.
Protocol	TCP, UDP, ICMP, IGMP, ESP, AH, ALL, or any other protocol defined in the Protocols section can be selected to match against the packet. If ALL is selected, no destination or source ports may be specified. Only TCP, UDP and ICMP can be used for a Deny filter using NAT.
Priority	A notice sent with the alarm event based on Unix syslog designations: 0=emergency; 1=alert; 2= critical; 3=error; 4=warning; 5=notice; 6=information; and 7=debug.
Authentication	Require authorized users to authenticate using GBAuth.
Actions	Select which actions will generate a notification: Alarm, Email, ICMP, Pager, SNMP, Stop Interface.
Log	Yes, No, and Default, as defined in Filter Preferences.
Time based Time group is	Select to make the filter operate at a specified time. Select time parameters.
Source Address	Packet IP address, alias or object will be matched against the source IP address of the packet.
Range	Specify a range of source ports.

Source Ports	The source port can be a single port or multiple ports Specified ports are matched against the source port of the IP packet. The source port for most client protocols is a random value above 1024. Leave blank to leave the port unspecified.
Destination Address	Packet IP address, alias or object will be matched against the packet destination IP address.
Range	Specify a range of ports.
Broadcast	Select if this is a Broadcast Destination.
Destination Ports	Often called services. Services were assigned dedicated port numbers ranging from 1 to 1024, but services have since been assigned outside this range.

Filter Preferences

Filter Preferences allow the user to globally set many logging and filter options in one location. See the Appendix for example log messages.

Logging

Filter and logging preferences have been consolidated in the Filter Preferences section, and logging options for automatic filters, tunnel connections (“opens” and “closes”), and filter blocks have been added. Default logging options are used when the **Default** option is selected in a filter definition LOG field, allowing the event selected to be logged whenever the filter is activated. All protocols are logged.

GTA Firewalls can now log the ICMP packets dropped by Stealth mode when Stealth logging is enabled.

Automatic filters are generated by the firewall to allow expected events such as response packets from DNS queries and mail servers. Automatic filters can be logged and disabled. GTA recommends disabling automatic filters only for troubleshooting and configuration testing.

Preferences Fields – General

Automatic Filters	Options: Enable/Disable; Log.
Deny address spoof	Always enabled. Options: Alarm, Email, Log. A spoof occurs when a packet arrives at one interface and its return path is through a different interface. This may be caused by an intrusion attempt made altering the packet source IP address; or a mis-configured firewall, e.g., when networks or hosts located on, or connected to, the internal side of a firewall have not been defined.
Deny doorknob twist	Always enabled. Options: Alarm, Email, ICMP, Log. A doorknob twist occurs when a connection is attempted on a port for which there is no service or tunnel in place and a filter has accepted the packet. A Doorknob Twist usually indicates that the firewall is mis-configured.
Deny fragmented packets	Options: Enable/Disable, Log. This option can be used to block some fragment attacks. By default, fragmented packets are reassembled and forwarded only if the resulting packet does not violate security policies; otherwise, they are dropped.
Deny invalid packets	Always enabled. Option: Log packets. If a packet is not the expected size or has an invalid option bit, the firewall denies the packet, e.g., an ICMP port unreachable packet must have at least 28 bytes. Invalid packets are dropped silently by default, but the system now includes the ability to log dropped packets.
Deny unexpected packets	Always enabled. Option: Enable/Disable, Log. If a packet is valid, but not expected by the state table, the firewall denies it, e.g., a packet can only generate a single ICMP port unreachable response; a second one may indicate an ICMP replay attack; also, an unexpected packet may be a packet that does not have the correct flags during TCP's three-way handshake. The system now includes the ability to log these packets.
Stealth Mode	Options: Enable/Disable, Log. Stealth mode has priority over other filters. Filters that allow pings, traceroutes, etc., from the External interface are not functional when the firewall is in stealth mode.
Default Logging	
Filter Blocks	Always enabled. Option: Log, enabled by default.
Tunnel Opens	Always enabled. Option: Log, disabled by default.
Tunnel Closes	Always enabled. Option: Log, enabled by default. Refer to tunnels created by the action of a filter (automatic or user-defined) or an inbound tunnel.

GNAT-Box Preferences

General

	Enable	Action to generate			
		Alarm	Email	ICMP	Log
Automatic filters:	☑				☐
Deny address spoof:	yes	☑	☐		☑
Deny doorknob twist:	yes	☑	☐	☐	☑
Deny fragmented packets:	☐				☐
Deny invalid packets:	yes				☐
Deny unexpected packets:	yes				☐
Stealth mode:	☑				☐
Default Logging					
Filter blocks:	yes				☑
Tunnel opens:	yes				☐
Tunnel closes:	yes				☑

Alarms

Threshold for generating email:	10 alarms
Threshold interval:	120 seconds
Maximum alarms per email:	500
Attempt to log host names:	☐
Page when threshold reached:	☐

Email Server

Enable:	☐
Server:	mailhost
From:	
To:	postmaster

SNMP Traps

Enable:	☐
Manager:	

Pager

Enable:	☐
COM port:	2
Speed:	4800
Phone number:	
Code:	,,,,,,1234#

Default | Save | Reset

Filter Preferences

7 NAT

Network Address Translation translates an IP address behind the firewall to that of the External Network interface, disguising the original and allowing the use of non-registered IP addresses within Protected Networks and PSNs, while still presenting registered IP addresses to the External Network.

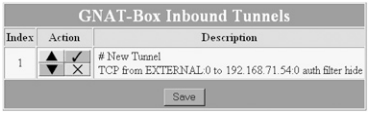
NAT and the NAT section have been updated to include:

- **Expanded inbound tunnel configuration**
- **Disable option for inbound tunnels**
- **Description field for inbound tunnels**
- **User authentication for inbound tunnels**

Inbound Tunnels

The Inbound Tunnels facility allows a host on an external network to be able to initiate a protocol from the Protocol List, e.g., TCP, UDP, ICMP, IGMP, ESP or AH session, with an otherwise inaccessible host, for a specific service.

Configuration has been updated to resemble the Filters section, with an initial list of tunnels with descriptions and Add, Edit and Delete icons.



Tunnel List

On the configuration screen, three additional fields, Disable, Description and Authentication Required, add functionality to Inbound Tunnels.

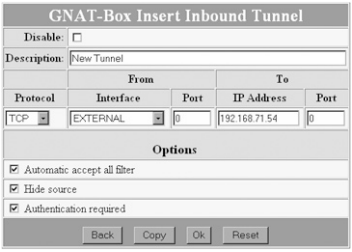
The Disable field allows the user to leave a tunnel definition in place, but not enable it until desired. The Description field gives the user the ability to identify the tunnel by a name or precise description.

Users whose information has been entered in User Authentication can now be required to enter a user name and password when accessing the firewall using

a filter or an inbound tunnel. See Chapter 9 – Utilities for more information about GBAuth.

Inbound Tunnel Fields

Disable	Disable a tunnel without deleting the definition.
Description	Word or phrase that clearly describes the tunnel.
Protocol	Protocol this tunnel will use: ALL, TCP, UDP, ICMP, IGMP, ESP, AH, etc.
From IP address	Interface object representing a network interface, an IP alias or a H_2A (high availability) group for the source side of the tunnel.
From Port	Port value which users will access. For an exhaustive list of ports and services, see www.iana.org/assignments/port-numbers on the IANA website.
To IP address	IP address of the target host. The host may reside on either the PSN or the Protected Network, including subnets routed behind either network.
To Port	Port which will be the destination of the tunnel. The port value is that of the service offered on the target host.
Automatic Accept All Filters	Make the tunnel connection ignore conflicting filters.
Authentication	Check to require the users allowed access with this filter to authenticate to the firewall using the GBAuth utility.
Hide Source	Hide the source of the inbound tunnel connection.



Tunnel Configuration

8 System Activity

The System Activity reports reflect the changes introduced in GNAT Box System Software to logging, filters, authentication, and log messages. Additions to system activity reports are:

- **Active Hosts (limited user license products)**
- **Authenticated Users**
- **View Log Messages**

Active Hosts

Active Hosts in System Activity helps track and regulate outbound access for systems with the number of concurrent user IP addresses restricted. The record includes the outbound user's IP address and the lease duration (time remaining). If the user continues to send outbound requests, remaining active, the lease will renew each time an outbound request is made. When the user is inactive, the lease time counts down, and if the user remains inactive for the timeout period, the lease duration column will report "expired," until the active lease limitation requires that license for another outbound user or the original user renews the lease. The duration of leases is defined as Timeouts under the NAT menu.

The number of licenses used is determined by the number of IP addresses from which outbound requests are currently being made. This includes IP addresses connecting from a Protected to External Network; Protected to PSN; PSN to External Network; and outbound connections opened by a Protected Network or PSN when responding to requests.

The Active Hosts screen appears only on systems with limited concurrent users. See you firewall's Basic Configuration – Features section or the GTA online support center for the number of concurrent users permitted by your GTA Firewall and optional features.

GNAT-Box Active Hosts		
Index	IP Address	Lease duration
1	10.10.1.82	expired

Active Host

Authenticated Users

The Authenticated Users report in System Activity helps track access by authenticated users. The record includes the outbound user's name as indicated in User Authorization, the source IP address and number of minutes the user has been active.

The last column, lease duration (time remaining), applies only mobile VPN users. If a VPN client user is actively connected, the lease will renew each time an outbound request is made. When the user is inactive, the lease time counts down, and if the user remains inactive for the timeout period, the lease duration column will report "expired," until the active lease limitation requires that license for another outbound user or the original user renews the lease. The duration of leases is defined as Timeouts under the NAT menu.

GNAT-Box Authenticated Users				
Index	Name	IP Address	Active	Lease duration
1	Mary	10.10.1.18	00:01:14	

Authenticated User

View Log Messages

Logging options have been included for automatic filters, packets received and sent, firewall startup, packet count, authenticated users and active hosts (limited user license products).

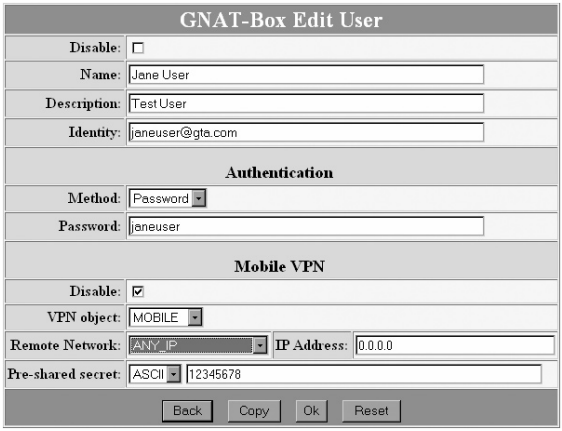
9 Utilities

GTA utilities are used for a variety of functions within GTA software, including GBAuth, the user authentication tool that provides an interface for users to authenticate to GTA firewalls; GTAsyslog, which replaces the functionality of the old syslog for all GTA software; DBmanager, which performs log server configuration, log imports, licensing and general database maintenance functions for GTA Reporting Suite and GMS (Global Management System); and LogView, which gives a user the ability to monitor the log messages from multiple firewalls remotely.

- **Additional functionality for GBAuth**
- **Added functionality for DBmanager (GB-DBMaint)**
- **GTAsyslog, GTA's improved logging tool (Syslog)**
- **Additional log viewing options using the new LogView**

GBAuth User Authentication

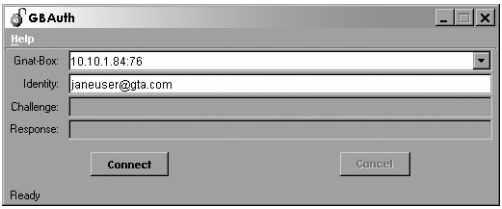
The GBAuth utility requires a user to enter a user identity and password set in GNAT Box System Software User Authorization.



User Authorization

If the Authentication Required checkbox has been selected on a filter, a user accessing the GTA Firewall using that filter must run GBAuth before initiating a connection.

Enter the name or IP address of the GTA Firewall in the GNAT Box field or select it from the drop-down box. Enter an identity (the email address specified in the GTA Firewall User Authorization section) in the Identity field, then click OK or press <Return>. The cursor will move to the Response field.



GBAuth

Enter the password from User Authorization, then click OK. If the identity or password is not recognized, an "Authentication failed" box will appear.

If the information is correct, a GBAuth lock icon appears in the system tray, and you can initiate a VPN connection through the firewall. By right-clicking on the GBAuth icon, you can display the authentication dialog, close the utility, or view the About box.

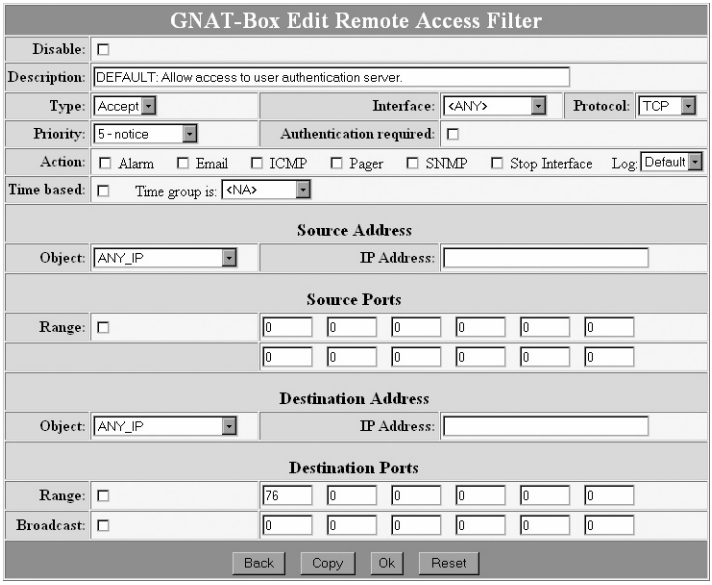
As long as the VPN is being used and data is being exchanged, the VPN automatically re-authenticates. If data is not being exchanged, the VPN closes after 10 minutes of inactivity. To close GBAuth and authentication, right-click on the icon and select Close.

Remote Access Filter

A default Remote Access Filter for mobile VPNs is set in the GNAT Box System Software. Once Mobile Authentication Required is checked, this filter can be enabled automatically by defaulting Remote Access Filters.

Note

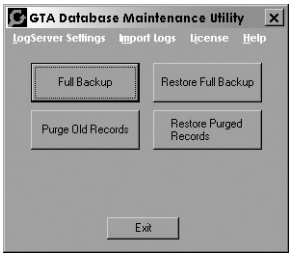
If filters have never been saved, they are auto-configured every time the system is restarted, according to the system parameters. If you have saved filters and then make changes to your GTA Firewall, using the Default button will auto-configure filters to match your system.



Mobile Authentication default filter

DBmanager

DBmanager is a utility for GTA software that helps maintain databases. It performs backups; purges data and restores data from backup files; configures the GTAsyslog; imports and exports from ODBC-compliant databases; and contains an interface for registering GTA Reporting Suite. Select DBmanager from the GTA sub-menu of Windows Start Menu.

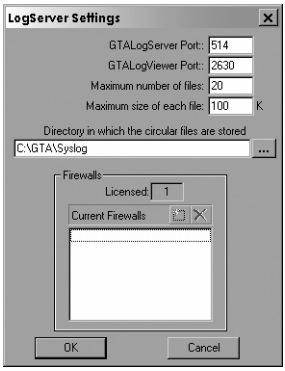


DBmanager

GTAsyslog

The GTAsyslog configuration dialog in DBmanager allows the user to select logging options–how the GTAsyslog and LogView utilities operate, and how Global Management System (GMS) and GTA Reporting Suite access recorded data.

The GTAsyslog automatically writes log data to a circular file which contains up to 1,000 log entries. Once at maximum, the file begins to overwrite log entries from the top.



GTAsyslog

GTAsyslog Fields	
GTAsyslog Port	Default – 514.
LogView Port	Default – 2630.
Maximum number of files	Consecutive log entries to retain before overwriting. Default – 20.
Maximum size of each file	Maximum file size for each log. Default – 100 K.
Log File Directory	Name of the data log file. Default – C:\GTA\syslog.
Current Firewalls	Host names of firewalls currently monitored by GTAsyslog. Firewalls can be added using the New Firewall icon if not yet added automatically; firewalls can be removed using the Delete icon.

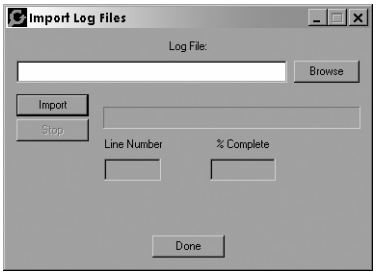
Import Logs

Select **Import Log Files** from the DBmanager menu to import GTA logs into the database or access log files from other sources. Click **Browse** and select one or more of the log files in **C:\gta\syslog** or from any other location where you have stored log files. Press the **<Control>** key while selecting file names to select more than one file. When you have selected one or more log files, click the **Import** button.

Use **Stop** to stop the database from continuing the import. The PROGRESS, LINE NUMBER and % COMPLETE fields give a calculation of the amount of the data that has been imported.

Note

When import is stopped then reselected, importing will start over.



Import Logs

Back Up and Restore Data

Regular backups and purging old records can be done on a daily, weekly or monthly basis, depending on corporate requirements. You may use the restore functions in case of a system failure or to search for evidence in a previously unrealized attack.

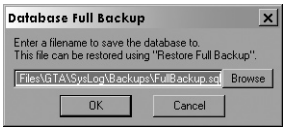
The options available from the selection screen are: Full Backup, Restore Full Backup, Purge Old Records and Restore Purged Records.

Note

GTA recommends storing full and incremental backups on a separate machine in a secure location. When using the same machine for backups, if the system fails, the backup files will be inaccessible.

Full Backup

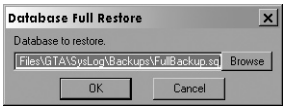
Using Full Backup allows the user to create a backup file of the current database (FullBackup.sql). The process also saves the registry settings to a separate file (FullBackup.reg). The database remains unchanged. A full backup does not remove any information.



Full Backup

Full Restore

A Full Restore of the database allows the user to select a file that copied the contents of the database at a specific time and return the entire backup to the database (FullBackup.sql). The process also restores the registry settings from a separate file (FullBackup.reg). The utility restores information exactly as it was at the selected Full Backup.



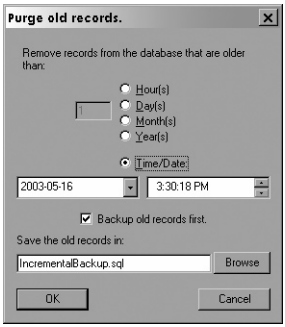
Restore Full Backup

Purge and Restore Data

Files backed up by Full Backup and Purge Old Records in GMS are named FullBackup.sql and IncrementalBackup.csv by default. As with all backup files, establish a file naming convention, and select a backup location other than the one where the server database is housed.

Purge Old Records

Purge Old Records is a utility that allows the user to delete selected alarm records from the database and create an incremental backup with this information (IncrementalBackup.csv). The user enters either the number of hours, days, months or years before which records should be purged, or the date before which records should be purged.



Purge Old Records

Restore Purge Records

Restore Purge Records is a utility that allows the user to restore records deleted from the database in an incremental backup (IncrementalBackup.csv).

Note

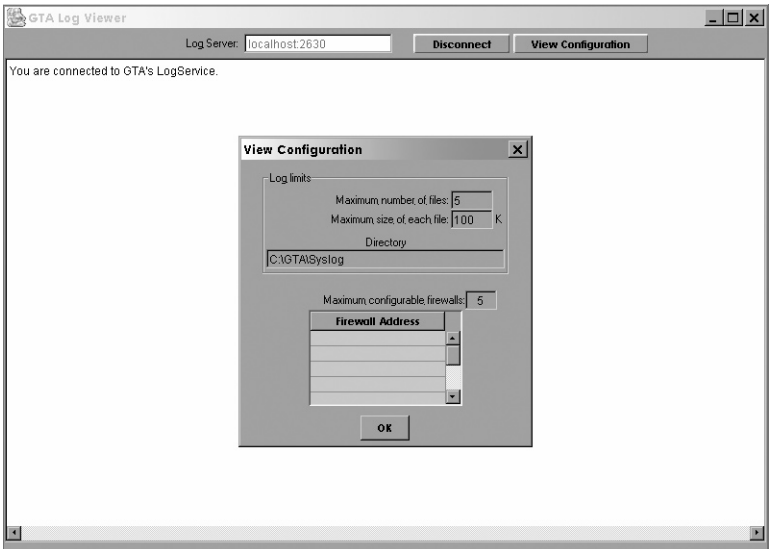
Purge Old Records (Incremental Backup) uses the Comma Separated Values (.csv) format.

LogView

LogView is a versatile viewer that gives read-only access to logs for up to 10 workstations. Only the main viewer installed with the GTAsyslog utility will able to manipulate log data; other workstations will have read-only access.

Users equipped with LogView can review log file data as it is written to the circular file from anywhere on the network. This facility does not maintain data beyond the log limit set in DBmanager.

Enter the location of your log files in the LOG SERVER field. By default, this is `localhost:2630`. Press <return> key to connect. Click the **Disconnect** button to stop viewing the log files.



Log Viewer with View Configuration

Appendix

Log Messages

Logging options have been added in for automatic filters, packets received and sent, firewall startup, packet count, authenticated users and active hosts (limited user license products).

For more examples of log messages, see the Appendix – Log Messages section in the **GNAT Box System Software User's Guide**.

Authenticated User

```
Jun 13 11:06:52 pri=6 msg="RMCauth: Allow 'support@gta.com',
authentication successful." type=mgmt src=192.178.71.254
srcport=3630 dst=10.10.1.84 dstport=76 duration=7 Jun 13 11:06:52
pri=5 msg="AUTH: Assign 192.178.71.254, to 'Mary'" type=mgmt Jun
13 11:06:46 pri=5 msg="RMCauth: Accepted connection" type=mgmt
src=192.178.71.254 srcport=3630 dst=10.10.1.84 dstport=76 duration=1
```

Authenticated User Close

```
Jun 13 11:18:00 pri=5 msg="RMCauth: Close connection" type=mgmt
src=192.178.71.254 srcport=3630 dst=10.10.1.84 dstport=76 dura-
tion=675 Jun 13 11:18:00 pri=5 msg="AUTH: Release 192.178.71.254,
from 'Mary'" type=mgmt
```

Authenticated User Denied

```
Jun 13 11:04:39 pri=5 msg="RMCauth: Close connection"
type=mgmt src=192.178.71.254 srcport=3569 dst=10.10.1.84
dstport=76 duration=17 Jun 13 11:04:38 pri=4 msg="RMCauth:
Deny 'support@gta.com', authentication failure." type=mgmt
src=192.178.71.254 srcport=3569 dst=10.10.1.84 dstport=76 dura-
tion=16 Jun 13 11:04:22 pri=5 msg="RMCauth: Accepted connection"
type=mgmt src=192.178.71.254 srcport=3569 dst=10.10.1.84 dstport=76
```

Tunnel Access after Authentication

```
Jan 6 17:36:04 pri=5 msg="Open inbound, NAT tunnel" proto=smtp
src=199.120.225.20 srcport=1806 user="Nick" nat=199.120.225.78
natport=25 dnat=10.10.1.78 dnatport=1806 dst=10.10.1.9 dstport=25
rule=1
```

Remote Access Filter without Authentication

```
Jun 4 13:27:08 pri=4 flt _ type=RAF flt _ action=block msg="Rejecting
unathenticated access (1)" rule=1 proto=25/tcp src=199.120.225.77
srcport=1700 dst=199.120.225.78 dstport=25 interface=sis1 flags=0x2
```

Remote Access Filter with Authentication

```
Jun 4 13:31:50 pri=5 msg="Open inbound, NAT tunnel" proto=smtp
src=199.120.225.77 srcport=1753 user="Nick" nat=199.120.225.78
natport=25 dnat=10.10.1.78 dnatport=1753 dst=10.10.1.9 dstport=25
rule=1
```

Attempt at Mobile VPN Without Authentication

```
Jan 11 14:20:09 pri=4 msg="Authentication needed, access for
'support@gta.com' denied." type=mgmt,vpn src=65.33.234.134
dst=199.120.225.78
```

Released User

User must authenticate again to gain access to restricted areas.

```
Jan 6 17:59:19 pri=5 msg="USER: Release 199.120.225.20, from
'Nick'" type=mgmt
```

Automatic Filters

Automatic Accept All filters can be logged by activating Automatic Filter logging in Filter Preferences. When activated, automatic filters will be recorded in the Active Filters table of the System Activity section.

```
Automatic Filter Example - Dec 2 10:23:33 pdbtest78.gta.com
FILTER: ATF (5) accept - notice ICMP [192.168.1.12:3]-
>[192.1168.1.78:3] fxp0 l=32 f=0x3.
```

Invalid Packets

```
Dec 2 10:30:59 pdbtest78.gta.com FILTER: Rejecting invalid packet:
warning TCP [10.10.1.98:0]->[10.10.1.78:0] fxp0 l=20 f=0x0
```

Active Host

```
Jan 9 01:14:22 pri=5 msg="Accept outbound, NAT" cat _ action=pass
dstname=www.eweek.com proto=http src=10.10.1.82 srcport=1658
nat=199.120.225.72 natport=1658 dst=63.87.252.160 dstport=80 rule=2
duration=349 sent=2480 rcvd=11842 pkts _ sent=18 pkts _ rcvd=17
op=GET arg=/util/css/eweek.css Jan 9 01:14:07 pri=5 msg="Accept
outbound, NAT" cat _ action=pass dstname=www.eweek.com proto=http
src=10.10.1.82 srcport=1657 nat=199.120.225.72 natport=1657
dst=63.87.252.160 dstport=80 rule=2 duration=334 sent=2709
rcvd=24433 pkts _ sent=24 pkts _ rcvd=25 op=GET arg=/print _
article/0,3668,a
```

Access Control List with Surf Sentinel Allowed

```
Oct 29 14:24:18 acmefirewall id=firewall time="2002-10-29 14:24:18"
fw="acmefirewall-ha-1" pri=5 msg="Accept outbound NAT"
cat _ action=pass cat _ site="Web Communications"
dstname=www.leadcart.com proto=http src=192.168.71.97 srcport=2661
nat=199.120.225.3 natport=2661 dst=205.138.3.133 dstport=80 rule=2
duration=23 sent=536 rcvd=537 pkts _ sent=6 pkts _ rcvd=5 op=GET
arg=/ads1/images/digits/n7.gif
```

Local Content List Denied

```
Oct 29 14:24:26 acmefirewall id=firewall time="2002-10-29 14:24:26"
fw="acmefirewall-ha-1" pri=4 msg="Block outbound NAT"
cat _ action=block cat _ site="Local Deny" dstname=ad.doublclk.net
proto=http src=src=192.168.71.33 srcport=4991 nat=199.20.136.33
natport=4991 dst=205.138.3.82 dstport=80 rule=2 duration=22
sent=861 rcvd=60 pkts _ sent=3 pkts _ rcvd=1 op=GET arg=/adi/
caranddriver.lana.com/kw=;;ord=180587622710292244
```

Index