

Technical Document

TD VPN-GB-MAC-03

GNAT Box[®] VPN

with IP Securitas from Lobotomo Software

GTA Firewall – Mac OS X

Configuring an IPSec VPN with IKE

GTA Firewall Software version 3.4

Mac OS X 10.2

IPSecuritas 1.1b2

Introduction	3
Mac OS X Configuration Using IPSecuritas	3
Create a New Connection	3
General Tab	4
Phase 1 Tab	5
Phase 2 Tab	5
ID/Auth Tab	6
Options Tab	7
Connect to the VPN	7

Copyright

© 1996-2003, Global Technology Associates, Incorporated (GTA). All rights reserved.

Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

Configuring an IPSec VPN with IKE from Mac OS X to a GTA Firewall

October 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 & Copyrights

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

Microsoft, Internet Explorer and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. WELF and WebTrends are trademarks of NetIQ. Sun, Sun Microsystems and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. The Java product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

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.

Introduction

GTA FIREWALL – MAC OS X: CONFIGURING AN IPSEC VPN is written for the administrator who requires a mobile VPN (virtual private network) to communicate from a Mac OS X system to the GTA Firewall. It is written with the assumption that the reader has a working knowledge of TCP/IP, Macintosh administration and GTA Firewall administration, including basic VPN configuration. This manual was developed using GNAT Box 3.4.0, Mac OS X 10.2 and IPSecuritas 1.1b2.

For GTA Firewall configuration of a mobile VPN, please see the **GNAT Box VPN AND VPN CLIENT FEATURE GUIDE**. Find this and other documented VPN setups, including interoperation with these vendors' solutions: Cisco PIX, NetScreen, WatchGuard, SonicWall and SnapGear, at www.gta.com/support2/documents.

VPN interoperability should be possible with any GTA Firewall that supports IKE. For the best support, the latest version of the GNAT Box Software is recommended.

Mac OS X Configuration Using IPSecuritas

Download IPSecuritas from Lobotomo Software at www.lobotomo.com and install on the Mac OS X system. IPSecuritas requires Mac OS X 10.2 (Jaguar) with the BSD subsystem installed. Configure the IPSecuritas client for a mobile VPN connection on Mac OS 10.2 using the following example.

Create a New Connection

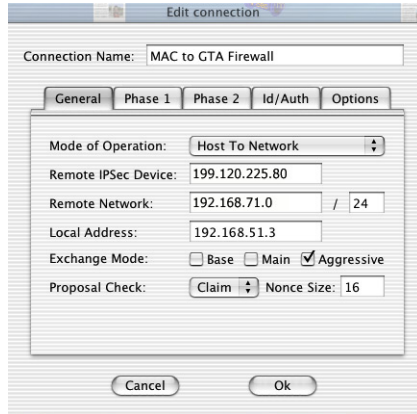
Start the IPSecuritas 1.1b2 application. Click on the **New** button to create a new VPN connection.



New VPN Connection

General Tab

In the **General** tab, use the following screen shot and table to enter the correct data, then select the **Phase 1** tab.



General

General

Connection Name	Enter a name for the connection.
Mode of Operation	Select Host to Network from the dropdown list.
Remote IPsec Device	Enter the external Interface IP address of the GTA Firewall.
Remote Network	Enter the network IP address to which the mobile client is to be connected, typically, the Protected Network of the GTA Firewall. This should match the LOCAL NETWORK field in the Mobile VPN Object definition of the GTA Firewall.
Local Address	Enter the virtual IP address used for the VPN. This must be a single IP address (not a network) and should match the IP address in the Mobile VPN section, REMOTE NETWORK field of Authorization/Users . This IP address should not be the same as the physical IP address assigned to the host, and, ideally, is on a different network and uses a private IP address.
Exchange Mode	Select Aggressive.
Proposal Check	Select Claim from the dropdown list.
Nonce Size	Enter 16.

Phase 1 Tab

In the **Phase 1** tab, use the following screen shot and table to enter the correct data, then select the **Phase 2** tab.

The **ENCRYPTION** and **AUTHENTICATION** fields should be set to match the fields in the Phase I section of the GTA Firewall Mobile VPN Object definition.



Phase 1

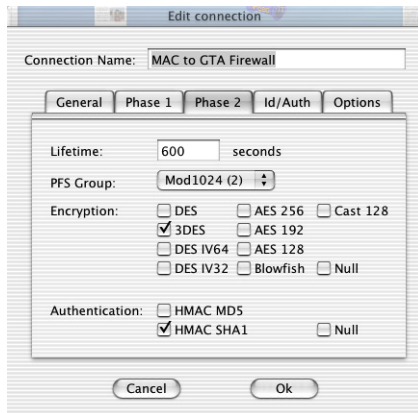
Phase 1

Lifetime	600 seconds.
DH Group	Mod1024 (2).
Encryption	3DES.
Authentication	SHA1.

Phase 2 Tab

In the **Phase 2** tab, use the following screen shot and table to enter the correct data, then select the **ID/Auth** tab.

The **ENCRYPTION** and **AUTHENTICATION** fields should be set to match the fields in the Phase II section of the GTA Firewall Mobile VPN Object definition.

*Phase 2*

Phase 2

Lifetime	600 seconds.
PFS Group	Mod1024 (2).
Encryption	3DES.
Authentication	HMAC SHA1.

ID/Auth Tab

In the **ID/Auth** tab, use the following screen shot and table to enter the correct data, then select the **Options** tab.

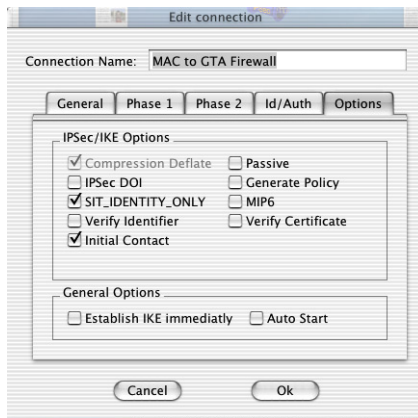
*ID/Auth*

ID/Auth

Local Identifier	Select DN. Enter an email address that matches the <code>IDENTITY</code> field in Authorization/Users on the GTA Firewall.
Remote Identifier	Select Address.
Preshared Secret	Enter the characters as in the <code>PRESHARED SECRET</code> field in Authorization/Users on the GTA Firewall.

Options Tab

In the **Options** tab, select only **SIT_IDENTITY_ONLY**, **Initial Contact** and **Compression Deflate** (greyed out), then select the **OK**.



Options

Connect to the VPN

Click the **Start IPsec** button. Once the IPsec is started, you should be able to connect through the VPN.