

Configuring GTA Firewalls for Mobile IPSec Clients

MIPSec201003-01



Global Technology Associates
3505 Lake Lynda Drive Suite 109
Orlando, FL 32817

Tel: +1.407.380.0220
Fax: +1.407.380.6080
Email: info@gta.com
Web: www.gta.com



Table of Contents

Introduction	1
IPSec Mobile Client Requirements	1
Firewall Configuration	1
Creating a Certificate Authority (CA) Certificate	1
Defining a Group	2
Defining Users	2
Configure Address Objects	3
Configure the Mobile IPSec Client	4
Configure Security Policies	5



Introduction

IPsec Mobile Client Requirements

- Mobile IPsec Client License
- IPsec Client (Shrew Soft VPN Client for Windows and Linux or IPsecrity IPsec Client for Mac)
- GB-OS 5.3.1 or higher

Firewall Configuration

Configuring the firewall for Mobile IPsec Clients involves six (6) steps:

1. Create a Certificate Authority (CA) certificate
2. Define a group
3. Define a user
4. Configure address objects
5. Configure the Mobile IPsec Client
6. Configure security policies

After configuring the firewall, the Mobile IPsec Client can be installed. Please see the specific Windows, Linux, and Mac OS guides for installing the Mobile IPsec Client.

Creating a Certificate Authority (CA) Certificate

Create a Certificate Authority (CA) Certificate to sign all other Certificates.

1. Navigate to **Configure>VPN>Certificates**.
2. Set the section to default. The firewall will automatically generate a new CA and Remote Administration certificate, and assign them as CA, Remote Administration, and VPN certificate. Below is an example of the CA, Remote Administration, and VPN certificates.

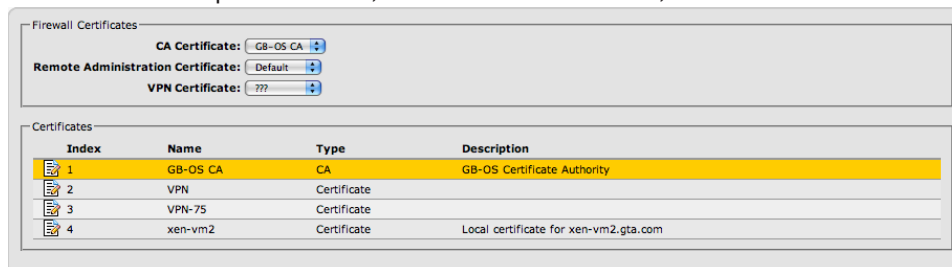


Figure 1: Creating Certificates



Note

See the *GB-OS Users Guide* for more information on creating firewall certificates.



Defining a Group

1. Navigate to **Configure>Accounts>Groups**.
2. Create a **NEW** group, or edit an existing group.
3. Enable Mobile IPSec.
3. Click **OK** and save section.

Figure 2: Defining a Group

Table 1: Defining Groups		
Field	Default	Description
Disable	Unchecked	Disables the group.
Name	Blank	Name used to reference the group for permissions.
Mobile IPSec		
Enable	Unchecked	Enables IPSec Client connections for the group.
Advanced		
Authentication Required	Unchecked	User must authenticate using GBAuth prior to establishing the VPN.
Local Network	Unchecked	Override for local network configured in Configure>VPN>Remote Access>IPSec .

Defining Users

1. Navigate to **Configure>Accounts>Users**. Create a **NEW** user or **EDIT** an existing user.
2. Select the Mobile IPSec group previously configured.
3. Assign the VPN certificate previously defined or generate a new certificate.
4. Enter the password the user will use to login to the IPSec Mobile Client.
5. Enable Mobile IPSec by leaving the **DISABLE** button unchecked.
6. Select **HYBRID + XAUTH** authentication.



Note

User certificates used for the IPSec Client **MUST** be signed by a CA.

Figure 3: Defining Users



Table 2: Defining Users		
Field	Default	Description
Disable	Unchecked	Disables the user.
Identity	Blank	The name used to authenticate the connecting user. This must be a unique name. Minimum of three (3) characters.
Full Name	Blank	Name to identify the user. Minimum of three (3) characters.
Description	Blank	User defined description for the user.
Primary Group	Users	Primary group for specifying the type of access allowed for the IPSec Client. Also used in security policies for authentication.
Certificate	Generate	Generate automatically creates a user certificate based on user definition, or select a predefined certificate.
Authentication		
Password	Blank	Password for user to authenticate with the firewall. Minimum of four (4) characters.
Mobile IPSec		
Disable	Checked	Uncheck to enable Mobile IPSec for the user.
Authentication	Hybrid + XAUTH	The authentication method the user MUST use for IPSec VPN. Options include Hybrid + XAUTH (password required); Pre-Shared Key (authenticated via pre-shared key); RSA (authenticated via certificate); and RSA + XAUTH (authenticated via certificate and password).

Configure Address Objects

1. Navigate to **Configure>Objects>Address Objects**.
2. Configure address objects for the local network and the DHCP pool range. The local network is the network to which the client will connect, and the DHCP pool range will be assigned to the clients connecting to the firewall. The default DHCP Pool range is 192.168.73.0/24.

Figure 4: Local Network Address Object

Figure 5: DHCP Pool Address Object



Configure the Mobile IPsec Client

1. Navigate to **Configure>VPN>Remote Access>IPsec**.
2. Enable the client.
3. Select the IPsec Object specifying encryption and authentication used for the VPN.
4. Define the LOCAL NETWORK the client will connect to.
5. Define the POOL NETWORK representing the DHCP range which will apply to clients using Xauth.
6. Optionally, configure the DNS servers and WINS servers for the client connections.
7. Configure advanced options as necessary.

Figure 6: Configuring the IPsec Client

Table 3: Enable IPsec Client

Field	Default	Description
Client		
Enable	Unchecked	Enable or disable the IPsec Client. Allows dynamic connections to the firewall.
IPsec Object	IPsec Mobile	A selection for the IPsec Object to be used by the IPsec Client. Selecting <* EDIT *> allows for the configuration of a new IPsec Object.
Local Network	FW Network - Local	Select the host/subnetwork that should be accessible from the VPN. Select <* EDIT *> to define a new address object.
Pool Network	Pool - IPsec	Select the DHCP pool that will be assigned to connecting clients. Select <* EDIT *> to define a new address object. Default DHCP range of 192.168.73.0/24.
Name Server IP Address	Blank	DNS server(s) pushed to IPsec Client.
WINS Server IP Address	Blank	WINS server(s) pushed to IPsec Client.



Table 3: Enable IPSec Client		
Field	Default	Description
Advanced		
Override Host Name	Blank	Allows an administrator to override the default firewall host name, which is configured in Network Settings. Entry can be an IP address or a fully qualified host name. This address will be used to connect to the firewall and should be used whenever the host name assigned to the firewall is not resolvable.
Authentication		
Local Identity	Certificate	Firewall's identity used for mobile IPSec client connections. Options include IP Address, Domain, Email Address and Certificate.
Method		
Hybrid + XAUTH	Checked	Enable or disable Hybrid + XAUTH authentication. Requires User Login and Password
Pre-shared Secret	Unchecked	Enable or disable pre-shared secret authentication. Firewall's local identity must be IP address, Domain or Email address.
RSA	Unchecked	Enable or disable RSA authentication. Requires user to have a signed certificate
RSA + XAUTH	Unchecked	Enable or disable RSA + XAUTH authentication. Requires user to have a signed certificate, and a username and password.
Hybrid + XAUTH		
LDAPv3	Unchecked	Enables LDAP users.
RADIUS	Unchecked	Enables RADIUS users.
Login Banner		
Enable	Unchecked	Enable or disable the login banner message.
Message	Blank	Enter a message to be displayed upon logging into the IPSec Client.

Configure Security Policies

Configure the IPSec security policies based on your corporate security policy. Below is an example of the default IPSec security policies. All access is allowed to internal networks and pings are allowed to the internal protected interfaces.

Index	Service	Description
1	<PING>	Allow pings to firewall using VPNs. Accept notice ANY <PING> from <ANY_IP> to <FW Interfaces - ALL> trafficShaping Default weight 5 coalesce(all)
2	<HTTPS>	Allow access to firewall admin using VPNs. Accept notice ANY <HTTPS> from <ANY_IP> to <FW Interfaces - ALL> trafficShaping Default weight 5 coalesce(all)
3	<ANY_SERVICE>	Deny access to firewall using VPNs. Deny warning ANY <ANY_SERVICE> from <ANY_IP> to <FW Interfaces - ALL> coalesce(all)
4	<ANY_SERVICE>	Allow all other VPN access. Accept notice ANY <ANY_SERVICE> from <ANY_IP> to <ANY_IP> trafficShaping Default weight 5 coalesce(all)
5	<ANY_SERVICE>	Block with alarm everything. Deny warning ANY alarm <ANY_SERVICE> from <ANY_IP> to <ANY_IP> coalesce(all)

Figure 7: Configuring Security Policies



Copyright

© 1996-2010, 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.

Technical Support

GTA includes 30 days “up and running” installation support from the date of purchase. See GTA's Web site for more information. 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 Authorized GTA Channel Partner.

Tel: +1.407.380.0220 **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

GB-OS, Surf Sentinel, Mail Sentinel and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. GB Commander is a trademark of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

Some products include software developed by the OpenSSL Project (<http://www.openssl.org/>).

Mailshell and Mailshell Anti-Spam is a trademark of Mailshell Incorporated. Some products contain technology licensed from Mailshell Incorporated.

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