

Technical Document

TD VPN-GB-NS-04

GNAT Box[®] VPN and VPN Client

with SoftRemoteLT from SafeNet, Inc.

GTA Firewall – NetScreen-5XP™

Configuring an IPSec VPN with IKE

GTA Firewall Software version 3.4

NetScreen-5XP version 2.6.0r1.4

Introduction	3
GTA Firewall Example VPN Configuration	3
NetScreen Example VPN Configuration	3
Encryption Methods	4
GTA Firewall Configuration	4
VPN Object	4
VPN Authorization	5
Remote Access Filters	6
IP Pass Through Filters	6
NetScreen Configuration	8
Networks	8
Phase 1 and 2	10
VPN Gateway	12
IKE VPN	13
Access Policies	13

Copyright

© 1996-2004, 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 for GTA Firewall to NetScreen-5XP Rev. March 2004

Technical Support

GTA includes 30 days “up and running” installation support from the date of purchase. See GTA’s website 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 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 and Surf Sentinel are registered trademarks of Global Technology Associates, Incorporated. RoBoX, GB-Commander and GB-Ware 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/>. SurfControl is a registered trademark of SurfControl plc.

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, Chris Williamson.

Technical Consulting: David Brooks. **Documentation:** Mary Swanson.

GTA Firewall IPSec VPN to NetScreen-5XP

Introduction

GTA FIREWALL – NETSCREEN-5XP™: CONFIGURING AN IPSEC VPN is written for the administrator who has both of these systems operating on a network and requires a VPN (virtual private network) to communicate between the firewalls. It is written with the assumption that the reader has a working knowledge of TCP/IP, NetScreen and GTA Firewall administration, including basic VPN configuration. This manual was developed using GNAT Box System Software 3.4.0 and NetScreen-5XP version 2.6.0r1.4. The NetScreen system in these examples is in its default configuration except for VPN. For the best support, the latest version of GTA Firewall Software is recommended.

The **GNAT BOX VPN AND VPN CLIENT FEATURE GUIDE** is the main reference for GTA Firewall VPN configuration. See other documented VPN setups at www.gta.com, including interoperation with these vendors' solutions: Cisco PIX, Mac OS X, WatchGuard, SonicWall and SnapGear. VPN interoperability should be possible with any GTA Firewall that supports IKE.

GTA Firewall Example VPN Configuration

To configure a GTA Firewall for VPN, use GBAdmin or the Web Interface. The examples given in this documentation use GBAdmin. This guide uses the following IP addresses as examples for a GTA Firewall VPN configuration:

External Interface	199.120.225.76
Protected Network	192.168.1.0/24

NetScreen Example VPN Configuration

To configure the NetScreen-5XP, use the GUI. This guide uses the following IP addresses as examples for a NetScreen configuration:

NetScreen External Interface	199.120.225.90
NetScreen Protected Network	10.10.11.0/24

Encryption Methods

The PROPOSAL lifetime on a NetScreen configuration cannot be longer than 3600 seconds (1 hour) for the VPN to perform properly. If the SA life is greater than 3600 seconds, you MAY experience problems when the systems renegotiate the keys.

Common Encryption Methods

GTA Firewalls have a number of encryption algorithms that do not have corresponding methods on the NetScreen firewall. Use the encryption methods below, common to both firewall systems, to configure both firewalls for a VPN connection.

Mode	IKE
ESP	DES or 3DES (Triple DES)
Hash	MD5 or SHA-1
Key Group	Diffie-Hellman group 1, 2 or 5

GTA Firewall Configuration

In order to use the GTA Firewall VPN feature, four functional areas must be configured: VPN Objects, VPN Authorization, Remote Access Filters and IP Pass Through Filters. VPN objects are used as the basis for VPN authorization, forming a link between the GTA Firewall and another firewall. User Authorization allows a GTA Firewall to connect to and authenticate a mobile client user or dynamic system user.

Note

For more information and illustrations about configuring a GTA Firewall VPN, see the **GTA FIREWALL SOFTWARE USER'S GUIDE**.

VPN Object

Open **Objects > VPN Objects**. Use the field table below as an example for entering data into the VPN Object fields.

VPN Object Fields

Disable	Enable. (Uncheck).
Name	Enter a name for this object. (GTA Firewall - NetScreen VPN Object)
Description	Enter a description of the VPN object. (GTA Firewall - NetScreen IKE VPN Object)

Local Gateway	Select the interface object for the GTA Firewall External Interface. (199.120.225.76)
Local Network	Select the GTA Firewall Protected Interface object or select Use IP Address and enter an IP address. (192.168.1.0/24)
Require Mobile Authentication	Uncheck.
Force Mobile Protocol	Uncheck.

Phase I

Exchange Mode	Main.
Encryption (ESP)	DES.
Hash	MD5.
Key Group	Diffie-Hellman Group 2.

Phase II

Encryption (ESP)	DES.
Hash	MD5.
Key Group	Diffie-Hellman Group 2.

VPN Authorization

Open **Authorization > VPNs** and add a new VPN. In the Key Exchange Type dialog, select IKE. Select **OK**, then enter the information in the VPN Authorization fields.

VPN Object Fields—Example

Disable	Enable. (Uncheck.)
Key Exchange	IKE (Uneditable. Selected in the previous dialog.)
Description	Enter a description of the VPN object. (GTA Firewall - NetScreen VPN Authorization)
Identity	Leave blank.
VPN Object	Select the VPN object created previously. (GTA Firewall - NetScreen IKE VPN)
Remote Gateway	Select the IP address or object that references the NetScreen External Network interface. (199.120.225.90)
Remote Network	Select the IP Address or object that references the NetScreen Protected Network. (10.10.11.0/24)
Preshared Secret	Preshared secret/key entered on the NetScreen system. (Preshared keys must be the same on both systems.)

Remote Access Filters

When using IKE, two Remote Access filter are necessary; one for the ESP Tunnel (IP protocol 50) and the other to allow access for IKE on UDP/500.

1	Description	VPN: Allow ESP connections from GTA Firewall to NetScreen VPN.
	Type	Accept
	Priority	Notice
	Interface	ANY
	Protocol	50 (ESP)
	Source	199.120.225.90
	Source Port	Blank
	Destination	External interface object (199.120.225.76)
	Destination Port	Blank
2	Description	VPN: Allow IKE connections from GTA Firewall to NetScreen VPN.
	Type	Accept
	Priority	Notice
	Interface	ANY
	Protocol	UDP
	Source	199.120.225.90
	Source Port	Blank
	Destination	External interface object (199.120.225.76)
	Destination Port	500

IP Pass Through Filters

Example filters below allow all access between the NetScreen and GTA Firewall networks. Set filters according to your corporate security policy.

At a minimum, an IP Pass Through filter must be created that allows outbound access on the defined VPN. Depending on your security policy, the filter can be as simple as allowing any host on the local network outbound access to any remote host for any protocol at any time, or as narrow as limiting a specific local host outbound access to a specific remote host for a given protocol at a specific time.

Generally, in addition, an inbound IP Pass Through filter is created that allows the remote side of the VPN access to the local Protected Network. This filter does not have to be symmetrical to the outbound IP Pass through filter, but rather should be created to meet the local security policy.

Typically, single inbound and outbound IP Pass Through filters are created for a VPN, but multiple filters may be required to make access conform to the local security policy.

1	Description	VPN: Allow inbound connections from GTA Firewall to NetScreen VPN.
	Type	Accept
	Priority	Notice
	Interface	External
	Protocol	ANY
	Source	10.10.11.0/24
	Source Port	Blank
	Destination	192.168.1.0/24
	Destination Port	Blank
2	Description	VPN: Allow outbound connections GTA Firewall to NetScreen VPN.
	Type	Accept
	Priority	Notice
	Interface	Protected
	Protocol	ANY
	Source	192.168.1.0/24
	Source Port	Blank
	Destination	10.10.11.0/24
	Destination Port	Blank

Note

Wherever an IP address is used in the filters, you can substitute an appropriate address object selected from the dropdown menu.

NetScreen Configuration

There are five parts to setting up a VPN on a NetScreen firewall to a GTA Firewall system:

- Define the NetScreen and GTA Firewall Protected networks.
- Define Phase 1 and Phase 2 policies for the VPN.
- Define the VPN gateway.
- Define the IKE VPN.
- Define Access Policies.

For more information on NetScreen VPN set up please see NetScreen support.

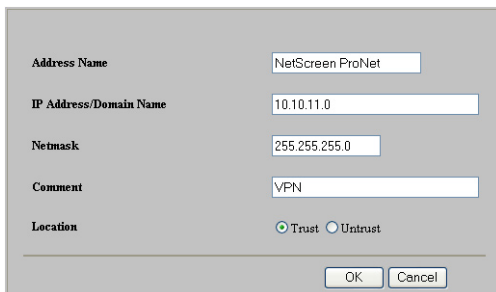
Networks

NetScreen devices define all other systems as addresses. Under **List > Addresses**, you will need to define two new addresses, one for the NetScreen-5XP protected network, and another for the GTA Firewall protected network.

NetScreen

To define the Protected Address of the NetScreen-5XP, go to **List > Address, Trusted** tab. Click **NEW ADDRESS**. Enter your network information using the following example, then click **OK**.

Address Name	NetScreen ProNet
IP Address/Domain Name	10.10.11.0 You cannot use domain names in making a VPN to a GTA Firewall.
Netmask	255.255.255.0
Comment	VPN
Location	Trust



The screenshot shows a configuration dialog box with the following fields and values:

Address Name	NetScreen ProNet
IP Address/Domain Name	10.10.11.0
Netmask	255.255.255.0
Comment	VPN
Location	<input checked="" type="radio"/> Trust <input type="radio"/> Untrust

At the bottom of the dialog are two buttons: **OK** and **Cancel**.

NetScreen Protected Network

Your Trusted list you should now look similar to the following:

Name	IP / Domain Name	Comment	Configure
Inside Any	0.0.0.0 / 0.0.0.0	All Trusted Addr	--
Netscreen ProNET	10.10.11.0 / 255.255.255.0	VPN	Edit

Trusted List

GTA Firewall

To define the Protected Address of the GTA Firewall go to **List > Address, UnTrusted** tab. Click **NEW ADDRESS**. Enter your network information using the following example, then click **OK**.

Address Name NetScreen ProNet
 IP Address/Domain Name 192.168.1.0 **You cannot use domain names in making a VPN to a GTA Firewall.**
 Netmask 255.255.255.0
 Comment VPN Network
 Location Untrust

Address Name: GB Protected Network
 IP Address/Domain Name: 192.168.1.0
 Netmask: 255.255.255.0
 Comment: VPN Network
 Location: Trust Untrust

OK Cancel

GTA Firewall Protected Network

Your Untrusted list you should now look similar to the following:

Name	IP / Domain Name	Comment	Configure
Outside Any	0.0.0.0 / 0.0.0.0	All Untrusted Addr	--
Dial-Up VPN	Dial-Up VPN Addr	--	--
GB Protected Network	192.168.1.0 / 255.255.255.0	VPN Network	Edit

Untrusted List

Phase 1 and 2

The NetScreen-5XP comes with several pre-defined proposals. GTA recommends creating your own proposals for phase 1 and phase 2 of the VPN.

Phase 1 Proposal

To define the Phase 1 Proposal, go to **Network > VPN**, and click on the **P1 Proposal** tab. Then click on **NEW PHASE 1 PROPOSAL**. Enter your network information using the following example, then click **OK**.

Name	GB > NetScreen
Authentication Method	Preshare
DH Group	Group 2
Encryption Algorithm	3DES-CBC
Hash Algorithm	SHA-1
Lifetime	1 Hour (maximum).

Note

A life time of more than 1 hour can cause the VPN to fail or not renegotiate the keys properly.

Phase 1

Your Phase 1 Proposal List should now have an entry for **GB > NetScreen** similar to the following:

Name	Method	DH Group	Encrypt/Auth.	Lifetime	Configure
dsa-g2-3des-md5	DSAsig	2	3DES / MD5	28800	--
dsa-g2-3des-sha	DSAsig	2	3DES / SHA	28800	--
GB -> NetScreen	Preshare	2	3DES / SHA	3600	Edit

Phase 1 Proposal List

Phase 2 Proposal

To define the Phase 2 Proposal, go to **Network > VPN**, and click on the **P2 Proposal** tab. Then click on **NEW PHASE 2 PROPOSAL**. Enter your network information using the following example, then click **OK**.

Name GB > NetScreen
 Perfect Forward Secrecy DH Group 2
 Encryption (ESP) Select
 Encryption Algorithm 3DES-CBC
 Authentication Algorithm SHA-1
 Lifetime 1 Hour (maximum).

Phase 2

Your Phase 2 Proposal List should now have an entry for **GB > NetScreen** similar to the following:

Name	PFS	Encap.	Encrypt/Auth.	Lifetime	Lifeseize	Configure
nopfs-esp-des-md5	No PFS	ESP	DES / MD5	3600	0	..
nopfs-esp-des-sha	No PFS	ESP	DES / SHA	3600	0	..
nopfs-esp-3des-md5	No PFS	ESP	3DES / MD5	3600	0	..
nopfs-esp-3des-sha	No PFS	ESP	3DES / SHA	3600	0	..
g2-esp-des-md5	DH Group 2	ESP	DES / MD5	3600	0	..
g2-esp-des-sha	DH Group 2	ESP	DES / SHA	3600	0	..
g2-esp-3des-md5	DH Group 2	ESP	3DES / MD5	3600	0	..
g2-esp-3des-sha	DH Group 2	ESP	3DES / SHA	3600	0	..
GB -> Netscreen	DH Group 2	ESP	3DES / SHA	3600	0	Edit

Phase 2 Proposal List

VPN Gateway

To define the VPN gateway, go to **Network > VPN** and click on the **Gateway** tab. Enter your network information using the following example, then click **OK**.

Gateway Name	GNAT Box Firewall External IP
Remote Gateway	Select the Static IP Address radio button and enter GTA Firewall External Interface IP address in our example, 199.120.225.76.
Mode (Initiator)	Main (ID Protection)
Phase 1 Proposal	Select the GB > NetScreen Proposal created in step 2.
Preshared Key	Match the key used on the GTA Firewall.
Preferred Certificate	None. (Not used.)

Note

You can use any proposal that matches the GTA Firewall. Verify that the Lifetime setting is not more than 1 hour.

VPN Gateway

Your gateway list should look similar to the following:

Name	Group/User Name/Peer IP	Peer ID	IKE Tunnel Type	Mode	P1 Proposals	Configure
GNAT Box Firewall External IP	199.120.225.76		PreShare	Main	GB -> NetScreen	Edit

Gateway List

IKE VPN

Go to **Network > VPN** and select the **AutoKey IKE** tab. Click on **NEW AUTOKEY IKE ENTRY**. Enter your network information using the following example, then click **OK**.

Name	GNAT Box to NetScreen
Enabled Replay Protection	Checked
Remote Gateway Tunnel	GNAT Box Firewall External IP gateway created in step 3.
Phase 2 Proposal	GB > NetScreen proposal defined in step 2.
VPN Monitor	Unchecked
Transport Mode	Unchecked

AutoKey IKE

Your AutoKey IKE list should look similar to the following:

Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure
GNAT Box to Netscreen	GNAT Box Firewall External IP	Yes	GB -> Netscreen	Off	Off	Edit

AutoKey IKE list

Access Policies

The policies are defined under **Network > Policy**. You will need to create two policies to allow traffic between the GTA Firewall and NetScreen protected networks, one for incoming traffic and one for outgoing traffic.

Outgoing Policy

The source and destination addresses have been defined earlier. Enter your network information using the following example, then click **OK**.

Name	VPN
Source Address	NetScreen ProNET
Destination Address	GB Protected Network
Service	ANY
NAT	Select Off radio button. NAT through the VPN may cause it to fail.
Action	Tunnel
VPN Tunnel	GNAT Box to NetScreen
L2TP	NONE
Logging	Enable
Counting	Unchecked
Authentication	Unchecked
Alarm Threshold	0 bytes/sec 0 bytes/min
Schedule	None
Traffic shaping	Off

The screenshot shows the configuration window for an Outgoing Policy. The settings are as follows:

- Name (optional):** VPN
- Source Address:** NetScreen ProNET
- Destination Address:** GB Protected Network
- Service:** ANY
- NAT:** Off (radio button selected)
- Action:** Tunnel
- VPN Tunnel:** GNAT Box to Netscreen
- L2TP:** None
- Authentication:** Unchecked
- Logging:** Enable (checked), Counting: Unchecked
- Alarm Threshold:** 0 Bytes/Sec, 0 Bytes/Min
- Schedule:** None
- Traffic Shaping:** Off (radio button selected)
- Traffic Shaping (when Off):**
 - Guaranteed Bandwidth: 0 kbps
 - Maximum Bandwidth: 0 kbps
 - Traffic Priority: Low priority
 - DS Codepoint Marking: Unchecked

Buttons for **OK** and **Cancel** are visible at the bottom right.

Outgoing Policy

Your Outgoing policy list should look similar to the following:

Incoming										Outgoing									
ID	Source	Destination	Service	NAT	Action	Option				Configure									
2	NetScreen ProNet	GB Protected Network	ANY	<input checked="" type="checkbox"/>							↑ Edit								
0	Inside Any	Outside Any	ANY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						↓ Edit								

Outgoing Policy List

Note

Order is important on the outgoing list. Be sure to move the VPN to the top of your list.

Incoming Policy

Enter your network information using the following example, then click **OK**.

- Name VPN
- Source Address GB Protected Network
- Destination Address NetScreen ProNET
- Service ANY
- NAT Select Off radio button. NAT through the VPN may cause it to fail.
- Action Tunnel
- VPN Tunnel GNAT Box to NetScreen
- L2TP NONE
- Logging Enable
- Counting Unchecked
- Authentication Unchecked
- Alarm Threshold 0 bytes/sec 0 bytes/min
- Schedule None
- Traffic shaping Off

Name (optional) VPN
Source Address GB Protected Network
Destination Address NetScreen ProNet
Service ANY
NAT Off
 DIP Off Fix-Port
 DIP On

Action Tunnel
VPN Tunnel GNAT Box to Netscreen
L2TP None

Authentication
Logging Enable **Counting** Enable

Alarm Threshold 0 Bytes/Sec 0 Bytes/Min

Schedule None

Traffic Shaping Off

kbps
 kbps
Traffic Priority Low priority
DS Codepoint Marking Enable

Incoming Policy

Note

Order is important on the Incoming list. Be sure to move the VPN to the top of your list.

Your GTA Firewall to NetScreen VPN should now be operational. To test the VPN, we recommend you ping from a host in the protected network defined on one system to the host on the protected network of the other.