

eSoft®

InstaGate IPsec VPN



Dynamic Remote Configuration

COPYRIGHT NOTICES

©eSoft Inc. 2008. eSoft, InstaGate, and ThreatWall are registered trademarks, and SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation. Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Inc. UNIX is a registered trademark of UNIX Systems Laboratories, Inc. All other brand and/or product names are the property of their respective holders.

Portions of this software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of this software are Copyright © The Regents of the University of California. A complete copy of the copyright notice follows:

Copyright © The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the University of California, Berkeley and its contributors.”

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

**THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS
“AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT
NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY**

AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software are Copyright © The Apache Group. A complete copy of the copyright notice follows:

Copyright © 1995-1997 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

INTRODUCTION

IPSec VPN's have become a highly used method of securely connecting geographically separate office locations together through an encrypted data tunnel. Dynamic IP addresses are still used by many ISP's making it necessary to configure an IPSec connection with a dynamic IP addresses. This guide will walk through how to configure eSoft InstaGate firewalls to connect via IPSec VPN when one end is on a dynamic IP address. It should be noted that one end of the IPSec tunnel must have a static IP address for this configuration. There is currently no way to configure an IPSec VPN tunnel between two dynamic IP devices.

PART ONE – DYNAMIC IP INSTAGATE CONFIGURATION

1.1 Access the IPSec VPN Menu

The Remote Office VPN settings are available in the InstaGate user interface under the firewall menu. After clicking the Remote Office VPN link, several options should now be available.

1.2 Adding a New IPSec Tunnel

To add a new IPSec tunnel click *Add*. The configuration of the Dynamic IP end of the tunnel is almost identical to the standard Pre-Shared Key configuration. On this page the IP Address information for both ends of the tunnel needs to be entered. Also the only Key Management type available for Dynamic Remote VPN tunnels is *Automatic (Shared Secret)*. Please note that the *Shared Secret* has to be identical on both ends of the tunnel.

1.3 IKE Settings

Once the main IPSec settings have been entered, click on the blue *IKE* button. On this page there will be a check box labeled *Aggressive Mode*. This setting tells the Dynamic Remote end to always be the unit to start the IPSec tunnel. Once enabled, some additional boxes will appear. These boxes contain Identifier information. This information is necessary to start an IPSec tunnel when one end does not have a static IP address. It is recommended that you use domains for local and remote identifiers. It is not necessary to use legitimate domains, fake domain names can be used in the identifiers field. Remember it is critical that the remote identifier match the local identifier of the unit on the other end of the tunnel.

1.4 Example Configuration

The screenshots below shows our final test configuration for the Dynamic IP Address side of an IPSec tunnel. Review the configuration settings below for our sample configuration. Some of these settings will be used in the configuration of the static IP end of the tunnel in Part Two.

- Local Network: 10.10.0.0/255.255.0.0
- Remote Gateway: 222.222.222.222
- Remote Network: 10.0.0.0/255.255.255.0
- Shared Secret: test

Firewall: Remote Office VPNs: Modify

IPSec VPN

Name: test Available Enabled

Network: Local Network to Remote Network Dynamic Remote Enabled

Key Management: Automatic (Shared Secret)

Network Settings

Local Host IP Address: WAN Interface

Local Network: 10.10.0.0 / 255.255.0.0

Remote Gateway IP Address: 222.222.222.222

Remote Network: 10.0.0.0 / 255.255.255.0

Key Management Settings

Shared Secret: test

IKE IPSec
Apply Cancel

1.5 IKE Settings

Review the configuration settings below for our sample configuration. Some of these settings will be used in the configuration of the static IP end of the tunnel in Part Two.

- IKE Aggressive Mode Enabled
- Local Identifier – Domain Name – DynamicInstagate.com
- Remote Identifier – Domain Name – StaticInstagate.com
- All other settings remain at default

Firewall: Remote Office VPNs: Modify: IKE: test ?

IKE Settings

Key Refresh or KB

Strict PFS Enabled

Aggressive Mode Enabled

Local Identifier

Type

Identifier

Remote Identifier

Type

Identifier

Proposals

Proposal

PART TWO – STATIC IP INSTAGATE CONFIGURATION

2.1 Access the IPSec VPN Menu

As stated in Section 1.1, the Remote Office VPN settings are available in the InstaGate user interface under the firewall menu.

2.2 Adding a New IPSec Tunnel

To add a new IPSec tunnel click *Add*. On the static end you must check the Dynamic Remote check box. Once this box has been selected you can now enter the Local and Remote Identifiers used previously. Please note that Local and Remote Identifiers should be reversed on each end of the tunnel.

2.3 Example Configuration

The screenshots below shows our final test configuration for the Static IP Address side of an IPSec tunnel. Review the configuration settings below for our sample configuration. Some of these settings will be used in the configuration of the static IP end of the tunnel in Part Two. Note that on the static end of the tunnel the IPSec settings do not need to be modified.

- Dynamic Remote is enabled
- Local Network: 10.0.0.0/255.255.255.0
- Local Identifier – Domain Name – StaticInstagate.com
- Remote Identifier – Domain Name – DynamicInstagate.com
- Remote Network: 10.10.0.0/255.255.0.0
- Shared Secret: test

Firewall: Remote Office VPNs: Modify

IPSec VPN

Name: test Available Enabled

Network: Local Network to Remote Network Dynamic Remote Enabled

Key Management: Automatic (Shared Secret)

Network Settings

Local Host IP Address: WAN Interface

Local Network: 10.0.0.0 / 255.255.255.0

Identifiers

Local Identifier

Type: Domain Name Identifier: StaticInstagate.com

Remote Identifier

Type: Domain Name Identifier: DynamicInstagate.com

Remote Network: 10.10.0.0 / 255.255.0.0

Key Management Settings

Shared Secret: test

IKE IPsec
Apply Cancel

TROUBLESHOOTING

There are logs available on your InstaGate. These logs are available through the user interface by going to Support and Diagnostics, System Logs. VPN information will be stored in the EVERYTHING.log. Please note that since one end of the IPSec tunnel is on a dynamic IP address, traffic needs to originate from the dynamic end in order for the IPSec tunnel to become active. Any tests run from the static end of the tunnel will fail to activate the IPSec tunnel.

Troubleshooting VPN connectivity problems can often be very complex. If you are unable to connect please open a ticket with eSoft Technical Support at 877-754-2986 or through online support at <http://support.esoft.com>.