

InstaGate EX™
Internet Security Appliance

DMZ SoftPak

Part Number: EX2-DMZ-093002

www.esoft.com

eSoft™

Copyright Notices

©eSoft, Inc. 2001. InstaGate, 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 InstaGate EX's 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 InstaGate EX's 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:

1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. 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."
4. 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 InstaGate EX’s 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:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. 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/>).”

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

5. 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/>).”





InstaGate EX SoftPak Demilitarized Zone (DMZ)

The DMZ SoftPak provides support for an additional Ethernet interface for hosting public servers on a network protected by the firewall, but isolated from the company LAN.

Connecting InstaGate EX to your DMZ Network

InstaGate EX is connected to your DMZ network like any other computer. The Ethernet DMZ Port automatically sets itself to the speed of your DMZ network (10 Mbps or 100 Mbps).

To connect InstaGate EX to your DMZ network:

1. Connect one end of a straight through CAT5 Ethernet cable (either of the two gray Ethernet cables provided) to the Ethernet DMZ Port on the back of InstaGate EX.

Note If you are using the internal DSL modem, internal analog modem, Euro ISDN, serial, synchronous serial V.35/X.21, or wireless 802.11B port rather than the Ethernet WAN port to connect to the Internet, and you do not have an Ethernet DMZ port installed, use the Ethernet WAN port as the DMZ interface.

2. Connect the other end of the Ethernet cable to a 10BASE-T or 100BASE-TX hub or switch on your DMZ network. Be sure to connect the Ethernet cable to a regular port on the hub, not an uplink port.

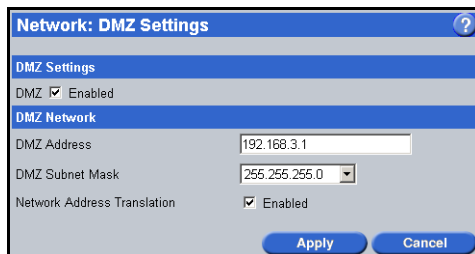
Configuring the DMZ Settings

DMZ adds a third network to InstaGate EX. The DMZ network is used for servers and other systems that must be accessible from the Internet, such as Web or FTP servers. The DMZ sits between the LAN and the Internet. While servers on the DMZ are publicly accessible, firewall protection can be enabled to protect the DMZ from Internet attacks. The LAN is always automatically protected from the DMZ.

Servers on the DMZ must have manually configured IP addresses, with the DMZ address as the default gateway.

To configure the DMZ settings:

1. Select *DMZ Settings* from the Network menu.
2. Click the *DMZ Enabled* check box.



3. Type the IP address of the DMZ interface in the *DMZ Address* text box. The DMZ interface can be on the same subnet as the WAN interface, or on a separate subnet. Configuring the DMZ interface on the same subnet as the WAN interface can be useful if the range of IP addresses assigned by your ISP is too small to divide into subnets.
4. Select the *DMZ Subnet Mask* used on the DMZ network (default 255.255.255.0). The subnet mask is used in conjunction with the DMZ IP address to define the set of addresses available on the DMZ.
5. Select the *Network Address Translation Enabled* (NAT) check box to activate NAT (and the firewall) on the DMZ network. NAT translates multiple IP addresses on the DMZ to one public address that is sent out to the Internet. This adds a level of security since the address of a system connected to the DMZ is never transmitted on the Internet. Internet access to servers on the DMZ is provided through defined firewall passthrough rules. DMZ servers are only protected by the firewall if NAT is enabled.

NAT protects DMZ servers from Internet attacks and only requires a single WAN IP address. The disadvantages of enabling NAT, however, are that only one DMZ server can provide a particular service, and that some services do not work well with NAT. Examples include popular messaging programs such as IRC and ICQ, and games that use Battle.Net or DirectPlay.

With NAT disabled, each DMZ server must have a unique Internet IP address. This eliminates the problems some services have with NAT, and allows multiple servers to provide the same service. However, without NAT, the DMZ servers are not protected by the firewall.

6. Click *Apply* to save your changes, or *Cancel* to exit without saving.