

eSoft

Simply better network security.™

®

**InstaGate®**

Firewall Policy Manager SoftPak

---

## Copyright Notices

©eSoft, Inc. 2003. eSoft and InstaGate 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 InstaGate'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'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’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 SoftPak Firewall Policy Manager

InstaGate EX's full-featured firewall provides your first and best level of defense against intrusion into your network. The firewall protects your network and Internet connection from malicious and inappropriate use by enforcing access policies you define.

## Accessing the Administration Utility

With the Firewall Policy Manager SoftPak installed, InstaGate uses Secure Sockets Layer (SSL) for connections to the administration utility.

SSL is a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

SSL achieves connection security through encryption and authentication. Encryption (128-bit) ensures that the connection between the server (InstaGate) and the client (browser) is private. Authentication (through a signed certificate) ensures the client that the server is who it says it is.

The certificate used to encrypt connections to the administration utility is automatically generated when you install the Firewall Policy Manager SoftPak.

To access the administration utility after installing the Firewall Policy Manager SoftPak:

1. Open a Web browser (Netscape Communicator 4.x or later or Internet Explorer 5.x or later).
2. In the address box, enter one of the following URLs:  
`https://<IPaddress_of_InstaGateEX>:8001`  
`https://Instagate:8001`
3. The SSL Certificate used to encrypt connections to the administration utility appears. You must accept the certificate to access the administration utility.

---

## Configuring Firewall Policies

A firewall policy is a set of parameters that define which services are available to your users and hosts. Use firewall policies to allow or deny communication in either direction between InstaGate and any or all IP addresses.

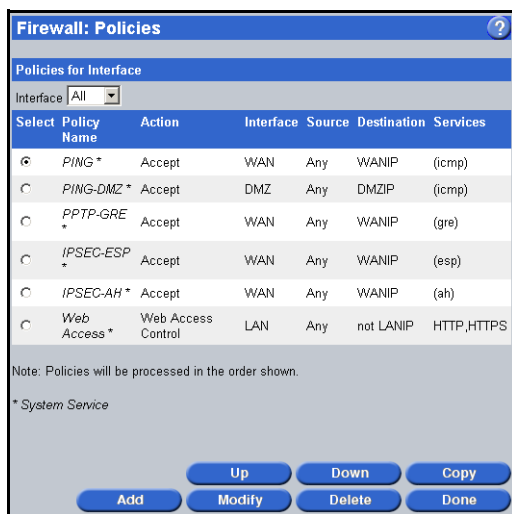
When an IP packet arrives, InstaGate EX checks the list of policies from top to bottom and uses the first policy it finds whose parameters match the IP packet. The IP packet must match the following parameters:

- Service being requested (SMTP, HTTP, etc.)
- Source address of the IP packet
- Destination address of the IP packet (optional)

Once it has chosen a policy, InstaGate EX checks the *Action* field to determine how the IP packet should be handled. If the Action field is set to *Accept*, the packet is allowed. If the Action field is set to *Deny*, the packet is dropped before any data is transferred. If the Action field is set to *Redirect*, the packet is accepted and passed to a specified destination. If the Action field is set to *Web Access Control*, the packet is accepted and passed to InstaGate's web caching proxy server.

To configure firewall policies:

1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears. You can view the policies which apply to the *LAN* interface, the policies which apply to the *WAN* interface, or *All* policies.



- 
2. To add a new firewall policy, click *Add*. See “Adding Firewall Policies” on page 8 for more information.

---

**Note** Any changes made to firewall policies (adding, modifying or deleting) are logged in the EVERYTHING.log file. To view the EVERYTHING.log file, select *System Logs* from the *Support and Diagnostics* menu, and select *General System* from the *Areas* drop-down list.

---

3. To modify an existing firewall policy, select the policy you wish to modify, and click *Modify*. See “Modifying Firewall Policies” on page 10 for more information.
4. To change the order of your firewall policies, select the policy you want to move, and click *Up* or *Down*.

When an IP packet arrives, InstaGate EX checks your policies list from top to bottom and selects the first policy that matches the source address and service requested. It is important, therefore, to list your policies in the correct order to prevent the wrong policy from being applied.

5. To remove an existing firewall policy, select the policy you want to remove, and click *Delete*. See “Deleting Firewall Policies” on page 10 for more information.
6. To create a copy of an existing firewall policy, select the policy you want to copy, and click *Copy*.

A copy of the selected policy is created with a unique name based on the name of the original. In order to preserve uniqueness, the word “copy” is appended to the name of the policy. If a policy with such a name already exists, a number is appended. That number is incremented until no matching policies are found. For example, if you try to copy a policy named “Block FTP”, and policies named “Block FTP copy” and “Block FTP copy 1” already exist, the new copy is named “Block FTP copy 2”.

7. Click *Done* when you have finished configuring firewall policies.

---

## Adding Firewall Policies

To add a new firewall policy:

1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears.
2. Click *Add*.

The screenshot shows the 'Firewall: Policies' configuration window. It is divided into three main sections:

- Policy Information:** Name: Remote Office Only; Action: Accept; Interface: WAN; Logging:  Enabled.
- Areas Affected:** Source IP or network address: 172.45.127.0; Destination IP or network address: WANIP.
- Services Affected:**  All services;  Select services. Under 'Select services', the following are checked:  HTTP,  HTTPS,  SMTP,  POP. Other services like DNS, FTP, LDAP, NNTP, and Telnet are unchecked.

Buttons at the bottom include 'Apply', 'Cancel', and 'Select Custom'.

3. Enter a *Name* for the policy.
4. Select the *Action* to take when an IP packet arrives matching the policy. To allow the packet, select *Accept*. To reject the packet, select *Deny*. To accept the packet and pass it to a specified destination, select *Redirect*. To accept the packet and pass it to InstaGate's Web Proxy Server, select *Web Access Control*.

---

**Note** Web Access Control rules only apply to HTTP and HTTPS requests from the LAN.

---

5. Select the *Interface* the policy applies to. To control access to the Internet by internal users, select *LAN*. To control access to your network by external users, select *WAN*. If you have downloaded and installed the DMZ SoftPak, select *DMZ* to control access to the LAN or WAN from servers on the DMZ network.
6. Select the *Logging Enabled* check box to log all connection attempts matching the policy. If you have *Web Access Control* selected in the Action field, logging is automatically enabled.

- 
7. Enter the IP address and subnet mask of the source host or network in the *Source IP or network address* fields. The source IP or network address refers to the IP address from which an IP packet originates. To apply the policy to packets originating from every IP address except the IP address (or range of addresses) specified in these fields, enter the address preceded by ~. For example, entering ~192.168.27.2 and 255.255.255.255 in the *Source IP or network address* fields applies the policy to packets originating from every IP address except 192.168.27.2.

---

**Note** If you frequently change InstaGate's LAN IP address or WAN IP address, you can enter **LANIP** or **WANIP** rather than the actual IP address to automatically update the policy whenever InstaGate's LAN IP address or WAN IP address change.

---

8. To restrict the policy to IP packets destined for a specific host or network, enter the IP address and subnet mask of the destination host or network in the *Destination IP or network address* fields. These fields are not available if you selected *Redirect* in the *Action* field. If these fields are left blank, the policy can apply to IP packets destined for any host or network. To apply the policy to packets destined for every IP address except the IP address (or range of addresses) specified in these fields, enter the address preceded by ~. For example, entering ~192.168.27.2 and 255.255.255.255 in the *Destination IP or network address* fields applies the policy to packets destined for every IP address except 192.168.27.2.
9. If you selected *Redirect* in the *Action* field, enter the *Destination IP (public address)* and the *Destination IP (internal address)*. For example, to redirect Internet service requests like Web (HTTP) or mail (SMTP) to a computer resource on your LAN, enter InstaGate EX's WAN IP address (192.168.1.1) in the public address field, and the IP address of the computer resource on your LAN that the request from the Internet should be forwarded to in the internal address field.  
  
The port and protocol for the destination IP addresses are determined by the *Service* selected.
10. Select the *Services Affected* by the policy. If the policy applies to all services, select the *All services* radio button. If the policy only applies to certain services, select the *Select services* radio button, and specify the services affected. Click *Select Custom* to specify any custom services affected (see "Setting up Custom Services" on page 10 for more information).
11. Click *Apply* to save the firewall policy, or *Cancel* to exit without saving.

---

## Modifying Firewall Policies

To modify a firewall policy:

1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears.
2. Select the policy you wish to modify, and click *Modify*.
3. Make any necessary changes to the policy.
4. Click *Modify* to save your changes.

## Deleting Firewall Policies

To delete a firewall policy:

1. Select *Policies* from the *Firewall* menu. A list of the policies currently defined on your system appears.
2. Select the policy you wish to delete, and click *Delete*.
3. Click *Delete* again to delete the firewall policy.

## Setting up Custom Services

InstaGate EX allows you to define custom Internet services. Access to these services can then be controlled through firewall policies.

To add a custom service:

1. Select *Custom Services* from the *Firewall* menu. A list of the services currently defined on your system appears. InstaGate EX automatically defines some of the more popular Internet services (AOL, IMAP, Lotus Notes, etc.)
2. Click *Add*.



The screenshot shows a dialog box titled "Firewall: Custom Services". Inside the dialog, there is a section labeled "Custom Service" with the following fields:

- Name: Time
- Protocol: TCP
- Source Port: (empty)
- Destination Port: 37

At the bottom right of the dialog are two buttons: "Apply" and "Cancel".

3. Enter a *Name* for the service.

- 
4. Select the *Protocol* of the service. A protocol is a standardized form of communication between network devices.

To specify a protocol that does not appear in the Protocol list, select *Other* and enter the *Protocol Number* (for example, **2** for igmp, **89** for ospf, or **94** for ipip).

5. If you selected *TCP* or *UDP* in the Protocol field, enter the network port number or the range of network port numbers to which requests for the service will connect. You can specify the *Source Port* number, the *Destination Port* number, or both. Enter port ranges in “x-y” format (for example, 23-25 or 8500-8599). The manufacturer of the software for which you are creating the custom service should be able to provide you with the port number the software uses.

If you selected *ICMP* in the Protocol field, enter the *Service number* for the custom service.

If you selected *GRE*, *AH*, or *ESP* in the Protocol field, no additional configuration is necessary.

---

**Note** For a list of common service ports and their protocols, as well as common ICMP messages and their service numbers, refer to the online help.

---

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

