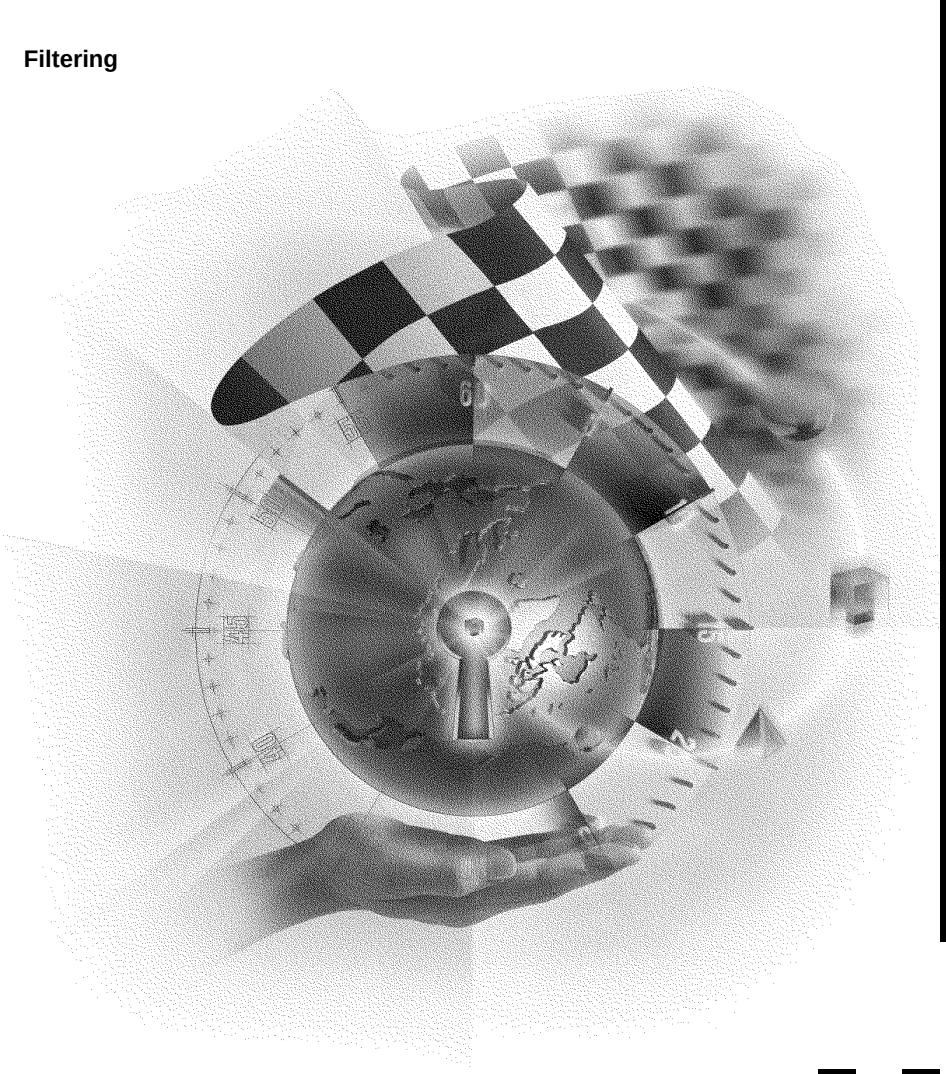
VERSION 3.5

Packet Filtering



BorderManager™

ENTERPRISE EDITION 3

Novell®

disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

The Harvest software was developed by the Internet Research Task Force Research Group on Resource Discovery (IRTF-RD):

Mic Bowman of Transarc Corporation.
Peter Danzig of the University of Southern California.
Darren R. Hardy of the University of Colorado at Boulder.
Udi Manber of the University of Arizona.
Michael F. Schwartz of the University of Colorado at Boulder.
Duane Wessels of the University of Colorado at Boulder.

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Packet Filtering
June 1999

TERMS OF USE

The Harvest software may be used and redistributed without charge, provided that the software origin and research team are cited in any use of the system. Most commonly, this is accomplished by including a link to the Harvest Home Page (http://harvest.cs.colorado.edu/) from the query page of any Broker you deploy, as well as in the query result pages. These links are generated automatically by the standard Broker software distribution.

The Harvest software is provided "as is," without express or implied warranty, and with no support nor obligation to assist in its use, correction, modification or enhancement. We assume no liability with respect to the infringement of copyrights, trade secrets, or any patents, and are not responsible for consequential damages. Proper use of the Harvest software is entirely the responsibility of the user.

DERIVATIVE WORKS

Users may make derivative works from the Harvest software, subject to the following constraints:

— You must include the above copyright notice and these accompanying paragraphs in all forms of derivative works, and any documentation and other materials related to such distribution and use must acknowledge that the software was developed at the above institutions.

— You must notify IRTF-RD regarding your distribution of the derivative work.

— You must clearly notify users that you are distributing a modified version and not the original Harvest software.

— Any derivative product is also subject to these copyright and use restrictions.

Note that the Harvest software is NOT in the public domain. We retain copyright, as specified above.

HISTORY OF FREE SOFTWARE STATUS

Originally we required sites to license the software in cases in which they were going to build commercial products/services around Harvest. In June 1995, we changed this policy. We now allow people to use the core Harvest software (the code found in the Harvest "src/" directory) for free. We made this change in the interest of encouraging the widest possible deployment of the technology. The Harvest software is really a reference implementation of a set of protocols and formats, some of which we intend to standardize. We encourage commercial reimplementation of code complying to this set of standards.

export notice

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

LANalyzer, LAN WorkPlace, Novell, and NetWare are registered trademarks of Novell, Inc. in the United States and other countries. BorderManager, Client 32, ConsoleOne, Internetwork Packet Exchange, IPX, NASI, NCP, NDPS, NDS, NetWare 5, NetWare Asynchronous Services Interface, NetWare Connect, NetWare Core Protocol, NetWare/IP, NetWare Link Services Protocol, NetWare Loadable Module, NetWare MultiProtocol Router, NLM, NLSP, Novell BorderManager, Novell BorderManager FastCache, Novell Client, Novell Distributed Print Services, Virtual Loadable Module, VLM, and Z.E.N.works are trademarks of Novell, Inc.

AppleTalk is a registered trademark of Apple Computer, Inc.

Btrieve is a registered trademark of Pervasive Software, Inc.

Cyber Patrol is a registered trademark of Learning Company Properties, Inc.

CyberNOT is a trademark of Learning Company Properties, Inc.

CyberNOT List is a trademark of Learning Company Properties, Inc.

CyberNOT is a trademark of Learning Company Properties, Inc.

CyberYES List is a trademark of Learning Company Properties, Inc.

Hayes is a registered trademark of Hayes Microcomputer Products, Inc.

Java is a trademark of Sun Microsystems, Inc. in the United States and other countries.

JavaScript is a trademark of Sun Microsystems, Inc.

Macintosh is a registered trademark of Apple Computer, Inc.

Microsoft is a registered trademark of Microsoft Corporation.

NCSA is a registered trademark of Bales, Gates & Associates, Inc.

Netscape is a registered trademark of Netscape Communications Corporation.

Netscape Communicator is a registered trademark of Netscape Communications Corporation.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

OS/2 is a registered trademark of International Business Machines Corporation.

PS/2 is a registered trademark of International Business Machines Corporation.

Pentium is a registered trademark of Intel Corporation.

RealAudio is a registered trademark of RealNetworks, Inc.

RealPlayer is a registered trademark of RealNetworks, Inc.

RealVideo is a registered trademark of RealNetworks, Inc.

The Learning Company is a registered trademark of Learning Company Properties, Inc.

UNIX is a registered trademark of X/Open Company, Ltd.

Contents

About This Guide

Novell® BorderManager™ Enterprise Edition 3.5 Installation and Setup provides the basic information you need to set up packet filters.

This documentation provides the following additional information:

- Chapter 1, “Advanced Configuration of IP Packet Filters,” on page 1

  This chapter describes how to set up HTTP, FTP, Telnet, SMTP, POP3, and DNS filters.

- Chapter 2, “Managing IP Packet Filters,” on page 15

  This chapter describes the configuration parameters for the IP packet filter log and the standard IP packet filter log format.

chapter

1 Advanced Configuration of IP Packet Filters

This chapter describes how to configure exceptions using FILTCFG to allow specific IP services through the Novell® BorderManager™ firewall when the action of the filters is to deny packets in the filter list. A server SET command to filter packets that have IP header options is also described.

This chapter contains the following sections:

Choosing between Stateful or Static Packet Filters

Stateful packet filters are more secure because they allow only the packets in response to requests to pass through the firewall. For this reason, the procedures in this chapter describe how to configure stateful packet filters. However, because static packet filters offer faster performance, a list of equivalent static filters is provided should you choose to configure them.

If you choose to configure static filters for the TCP protocol, you should enable ACK bit filtering so that all inbound packets that do not have the TCP ACK bit set are dropped by the server.

Setting Up an HTTP Filter

You can set up an HTTP filter on your server's public interface to filter HTTP packets in the inbound or outbound direction. An inbound HTTP filter might be required to allow public access to specific Web servers in your private network. An outbound HTTP filter might be required to allow certain users to bypass proxy services and connect directly to origin Web servers.

This section contains the following tasks:

- "Setting Up a Stateful HTTP Filter"
- "Setting Up Static Filters for HTTP"

Setting Up a Stateful HTTP Filter

To set up a stateful HTTP filter exception, complete the following steps from the main FILTCFG menu:

1. **Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.**
2. **Press** Ins **to define a new exception.**
3. **If you are creating an inbound exception, do the following:**
   - 3a. **Specify <All Interfaces> for the Source Interface parameter.**
   - 3b. **Specify the server's public interface for the Destination Interface parameter.**
   - 3c. **Press** Enter **for Packet Type and select www-http-st.**

Note The www-http-st packet type is for HTTP over TCP. This packet type will not work for HTTP over UDP.

   - 3d. **If you want the server to forward HTTP packets from certain public hosts only, specify Host or Network for the Src Addr Type parameter and enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.**

3e. If you want the server to forward HTTP packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter and enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

3f. Press Esc **and select Yes to save the filter.**

4. If you are creating an outbound exception, do the following:

4a. Specify the server's private interface for the Source Interface parameter.

4b. Specify the server's public interface for the Destination Interface parameter.

4c. Press Enter **for Packet Type and select www-http-st.**

4d. If you want the server to forward HTTP packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter and enter the IP address for Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

4e. If you want the server to forward HTTP packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter and enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

4f. Press Esc **and select Yes to save the filter.**

Important The outbound stateful HTTP filter does not allow packets for Domain Name System (DNS) name resolution to be forwarded to a DNS server on the public network. DNS names in URLs cannot be resolved unless you set up a DNS filter. Refer to "Setting Up a DNS Filter" on page 11.

Setting Up Static Filters for HTTP

If you do not want to configure a stateful HTTP exception, you can create static filters instead.

In the direction that HTTP requests will be sent, create one or both of the following static packet filter exceptions:

- www-http (for HTTP over TCP)

- www-http/udp (for HTTP over UDP)

Most browsers are configured to use HTTP over TCP, but they can also use HTTP over UDP. If you support browsers using HTTP over UDP, you should create both filters.

In the direction that HTTP responses will be sent, create one or both of the following static packet filter exceptions:

- dynamic/tcp (for HTTP over TCP)
- dynamic/udp (for HTTP over UDP)

The exceptions you create depend on which exceptions you created for the opposite direction of packet flow. If you created exceptions for both www-http and www-http/udp, you should create filter exceptions for both dynamic/tcp and dynamic/udp. The dynamic port range is 1024 to 65,535.

Important These filters do not allow packets for DNS name resolution to be forwarded. To set up a DNS filter, refer to “Setting Up a DNS Filter” on page 11.

Setting Up an FTP Filter

You can set up an FTP filter on your server’s public interface to filter FTP packets in the inbound or outbound direction. An inbound FTP filter might be required if public users connect to an FTP server in your private network. An outbound FTP filter might be required to allow certain users to bypass proxy services and connect directly to FTP servers on the public network.

When you set up an FTP filter, you can configure it to inspect for active FTP connections, passive FTP connections, or both. For tighter security, some administrators only allow active FTP connections in the inbound direction so the data connection is always on port 20. In contrast, passive FTP connections use any dynamic ports that are available.

This section contains the following tasks:

- “Setting Up a Stateful FTP Filter”
- “Setting Up Static Filters for FTP”

Setting Up a Stateful FTP Filter

To set up a stateful FTP filter exception, complete the following steps from the main FILTCFG menu:

1. **Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.**

2. **Press** Ins **to define a new exception.**

3. **If you are creating an inbound exception, do the following:**

   3a. Specify <All Interfaces> for the Source Interface parameter.

   3b. Specify the server's public interface for the Destination Interface parameter.

   3c. Press Enter **for Packet Type and select ftp-port-pasv-st.**

Note The packet type ftp-port-pasv-st allows both active and passive FTP connections. To allow active FTP connections only, select ftp-port-st. To allow passive FTP connections only, select ftp-pasv-st.

   3d. If you want the server to forward FTP packets from certain public hosts only, specify Host or Network for the Src Addr Type parameter and enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

   3e. If you want the server to forward FTP packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter and enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

   3f. Press Esc **and select Yes to save the filter.**

4. **If you are creating an outbound exception, do the following:**

   4a. Specify the server's private interface for the Source Interface parameter.

   4b. Specify the server's public interface for the Destination Interface parameter.

   4c. Press Enter **for Packet Type and select ftp-port-pasv-st.**

Note The packet type ftp-port-pasv-st allows both active and passive FTP connections. To allow active FTP connections only, select ftp-port-st. To allow passive FTP connections only, select ftp-pasv-st.

4d. If you want the server to forward FTP packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter and enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

4e. If you want the server to forward FTP packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter and enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

4f. Press Esc and select Yes to save the filter.

Important The outbound stateful FTP filter does not allow packets for DNS name resolution to be forwarded to a DNS server on the public network. Users establishing an FTP connection to an FTP server must use the FTP server's IP address unless you set up a DNS filter. Refer to "Setting Up a DNS Filter" on page 11.

Setting Up Static Filters for FTP

If you do not want to configure a stateful FTP exception, you can create static filters instead.

To allow public hosts to establish active FTP connections to a server in the private network, configure the following inbound and outbound filter exceptions:

- ftp (the control channel)
- ftp-data (the data channel)

If you want to allow users in your private network to establish passive FTP connections to public servers, configure additional filter exceptions for dynamic/tcp in both directions so dynamic ports can be used as the data channel instead of port 20. Enable ACK bit filtering for the dynamic/tcp exceptions.

Important These filters do not allow users to establish FTP connections using the FTP server's DNS name. A DNS filter is required. To set up a DNS filter, refer to "Setting Up a DNS Filter" on page 11.

Setting Up a Telnet Filter

You can set up a Telnet filter on your server's public interface to filter Telnet packets in the inbound or outbound direction. An inbound Telnet filter might be required if public users establish Telnet sessions to a server in your private network. An outbound Telnet filter might be required to allow users to establish a Telnet session on the public network.

This section contains the following tasks:

- "Setting Up a Stateful Telnet Filter"
- "Setting Up Static Filters for Telnet"

Setting Up a Stateful Telnet Filter

To set up a stateful Telnet filter exception, complete the following steps from the main FILTCFG menu:

1. **Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.**
2. **Press** Ins **to define a new exception.**
3. **If you are creating an inbound exception, do the following:**
   - **3a. Specify <All Interfaces> for the Source Interface parameter.**
   - **3b. Specify the server's public interface for the Destination Interface parameter.**
   - **3c. Press** Enter **for Packet Type and select telnet-st.**
   - **3d. If you want the server to forward Telnet packets from certain public hosts only, specify Host or Network for theSrc Addr Type parameter and enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.**
   - **3e. If you want the server to forward Telnet packets addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter and enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.**

3f. Press Esc and select Yes to save the filter.

4. If you are creating an outbound exception, do the following:

4a. Specify the server's private interface for the Source Interface parameter.

4b. Specify the server's public interface for the Destination Interface parameter.

4c. Press Enter for Packet Type and select telnet-st.

4d. If you want the server to forward Telnet packets from certain private hosts only, specify Host or Network for the Src Addr Type parameter and enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.

4e. If you want the server to forward Telnet packets addressed to certain public hosts only, specify Host or Network for the Dest Addr Type parameter and enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.

4f. Press Esc and select Yes to save the filter.

Important The outbound stateful Telnet filter does not allow packets for DNS name resolution to be forwarded to a DNS server on the public network. Users establishing a Telnet session must use IP addresses unless you set up a DNS filter. Refer to "Setting Up a DNS Filter" on page 11.

Setting Up Static Filters for Telnet

If you do not want to configure a stateful Telnet exception, you can create static filters instead. Simply create a static Telnet filter exception in both the inbound and outbound directions. Make sure you enable ACK bit filtering for the exception in the inbound direction.

Important These filters do not allow users to establish Telnet sessions using a server's DNS name. A DNS filter is required. To set up a DNS filter, refer to "Setting Up a DNS Filter" on page 11.

Setting Up an SMTP Filter

You can set up a Simple Mail Transfer Protocol (SMTP) exception on the server's public interface to allow SMTP mail servers or SMTP gateways in your private network to send and receive mail through the Novell® BorderManager™ firewall.

This section contains the following tasks:

- "Setting Up a Stateful SMTP Filter"
- "Setting Up Static Filters for SMTP"

Setting Up a Stateful SMTP Filter

To set up a stateful SMTP filter exception, complete the following steps from the main FILTCFG menu:

1. **Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.**
2. **Press** Ins **to define a new exception.**
3. **Specify the Source Interface by doing one of the following:**
   - 3a. **If you want private SMTP servers or gateways to be able to send mail through the firewall, specify the server's private interface.**
   - 3b. **If you want public SMTP servers to be able to send mail to the SMTP server in your private network, and you have not enabled the Mail proxy, specify the server's public interface.**
4. **Specify the Destination Interface by doing one of the following:**
   - 4a. **If you want private SMTP servers or gateways to be able to send mail through the firewall, specify the server's public interface.**
   - 4b. **If you want public SMTP servers to be able to send mail to the SMTP server in your private network, and you have not enabled the Mail proxy, specify the server's private interface.**
5. **Press** Enter **for Packet Type and select smtp-st.**

6. **Press** Esc **and select Yes to save the filter.**

Important The outbound stateful SMTP filter does not allow domain names to be resolved by a DNS server on the public network. Refer to “Setting Up a DNS Filter” on page 11.

Setting Up Static Filters for SMTP

If you do not want to configure a stateful SMTP exception, you can create static filters instead. Simply create a static SMTP filter exception in both the inbound and outbound directions. Make sure you enable ACK bit filtering for the exception in the inbound direction.

Important These filters do not forward requests for domain name resolution. A DNS filter is required. To set up a DNS filter, refer to “Setting Up a DNS Filter” on page 11.

Setting Up a POP3 Filter

You can set up a Post Office Protocol 3 (POP3) exception on the server’s public interface to allow public clients to access a private POP3 server behind the Novell® BorderManager™ firewall.

This section contains the following tasks:

- “Setting Up a Stateful POP3 Filter”
- “Setting Up a Static POP3 Filter”

Important These filters do not forward requests for domain name resolution by a DNS server in your private network. A DNS filter is required. To set up a DNS filter, refer to “Setting Up a DNS Filter” on page 11.

Setting Up a Stateful POP3 Filter

To set up a stateful POP3 filter exception, complete the following steps from the main FILTCFG menu:

1. **Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.**
2. **Press** Ins **to define a new exception.**
3. **Specify <All Interfaces> for the Source Interface parameter.**

4. **Specify the server's public interface for the Destination Interface parameter.**

5. **If you want the server to forward mail from certain public hosts only, specify Host or Network for the Src Addr Type parameter and enter the IP address for the Src IP Address parameter; otherwise, leave the setting for Src Addr Type as Any Address.**

6. **If you want the server to forward mail addressed to certain private hosts only, specify Host or Network for the Dest Addr Type parameter and enter the IP address for the Dest IP Address parameter; otherwise, leave the setting for Dest Addr Type as Any Address.**

7. **Press** Enter **for Packet Type and select pop3-st.**

8. **Press** Esc **and select Yes to save the filter.**

Setting Up a Static POP3 Filter

If you do not want to configure a stateful POP3 exception, you can create a static filter instead. Make sure you enable ACK bit filtering for the exception in the inbound direction.

Setting Up a DNS Filter

TCP/IP connections to a server can be made by specifying the server's IP address, but most servers, particularly those connected to the Internet, are accessed by their DNS names.

This section contains the following tasks:

- "Setting Up a Stateful DNS Filter"
- "Setting Up Static Filters for DNS"

Setting Up a Stateful DNS Filter

To set up a stateful DNS exception to allow users to use DNS names to connect to servers accessed through the Novell® BorderManager™ server's public interface, complete the following steps from the main FILTCFG menu:

1. **Select Configure TCP/IP Filters > Packet Forwarding Filters > Exceptions.**
2. **Press** Ins **to define a new exception.**
3. **Specify the server's private interface for the Source Interface parameter.**
4. **Specify the server's public interface for the Destination Interface parameter.**
5. **Press** Enter **for Packet Type and select dns/udp-st.**
6. **Press** Esc **and select Yes to save the filter.**

Important If applications are configured to use DNS over TCP, you can also configure a stateful DNS exception for DNS over TCP. In Step 5, select the dns/tcp-st packet type instead of the dns/udp-st packet type.

Setting Up Static Filters for DNS

If you do not want to configure a stateful DNS exception, you can create static filters instead.

In the direction that DNS queries will be sent, create the following static packet filter exception:

- dns/udp

In the direction that DNS responses will be sent, create the following static packet filter exception:

- dynamic/udp

Filtering IP Packets that Use the IP Header Options Field

In addition to containing 32-bit source IP address and destination IP address fields, IP packets also contain an options field. This field can be used for the following purposes:

- Security restrictions—United States Department of Defense (DoD) basic and extended security options to identify classification levels and secuirty information.
- Record route—List of IP addresses to identify each router that forwarded the packet.
- Time stamp—List of IP addresses and time stamps to identify each router that forwarded the packet.
- Source routing—List of IP addresses to which the packet must be routed.

Although the NetWare® TCP/IP stack does not process these options, it can be a security risk to forward packets with these options specified. In particular, the source routing option can force all packets that are routed from your network to be forwarded to an untrustworthy host in the public network.

When you install Novell® BorderManager™ firewall/caching services, a server SET command is automatically enabled to drop packets with IP header options enabled.

To view the current setting for your server, complete the following steps:

1. **At the server console, enter**

   SET

2. **Select option 1 (Communications).**

3. **Verify that the SET command displays as**

   SET FILTER PACKETS WITH IP HEADER OPTIONS = ON

It is best not to change the default setting, but under certain circumstances you might need to turn this setting off. For example, you could use the source routing option to specify the routers that must handle the traffic from your network.

Important Because routers often do not support IP header options, be sure to verify the capability of your routers before disabling the filtering to perform such tests.

To disable the filtering of packets that use IP header options from the server console, enter

SET FILTER PACKETS WITH IP HEADER OPTIONS = OFF

To reenable the filtering from the server console, enter

SET FILTER PACKETS WITH IP HEADER OPTIONS = ON

chapter

2 Managing IP Packet Filters

This chapter describes how to manage Novell® BorderManager™ IP packet filters used as part of your firewall. It contains the following sections:

Modifying Default IP Logging Parameters

If global logging for IP has been enabled, IP packets are automatically logged to a text file located in the SYS:ETC\LOGS\IPPKTLOG directory on the server. The configuration file, SYS:ETC\IPPKTLOG.CFG, specifies the logging parameters.

Important IP packets that match a specific packet filtering rule are not logged unless logging has been explicitly enabled for the filter.

Refer to Table 2-1 on page 16 for the logging configuration parameters in IPPKTLOG.CFG.

Table 2-1
IPPKTLOG.CFG Configuration Parameters

Parameter	Default Value	Available Settings
LOG_FILE_TYPE	1	1 = Sequential log file.
LOG_FILE_LOCATION	SYS:ETC\LOGS\IPPKTLOG	Any directory.
LOG_FILE_ROLL_METHOD	3	1 = Roll log file every *n* hours, where *n* is the value assigned to LOG_FILE_ROLL_METHOD_VALUE. 2 = Roll log file every *n* days, where *n* is the value assigned to LOG_FILE_ROLL_METHOD_VALUE. 3 = Roll log file when the log file size exceeds *n* KB, where *n* is the value assigned to LOG_FILE_ROLL_METHOD_VALUE.
LOG_FILE_ROLL_METHOD_VALUE	100	Any value representing hours when LOG_FILE_ROLL_METHOD is 1. Any value representing days when LOG_FILE_ROLL_METHOD is 2. Any value representing KB when LOG_FILE_ROLL_METHOD is 3.
LOG_FILE_DELETE_METHOD	2	1 = Do not delete log files. 2 = Begin deleting log files when the number of log files reaches the limit specified by LOG_FILE_DELETE_METHOD_VALUE. 3 = Begin deleting log files when the age of the log files reaches *n* hours, where *n* is the value assigned to LOG_FILE_DELETE_METHOD_VALUE.

Parameter	Default Value	Available Settings
LOG_FILE_DELETE_METHOD_VALUE	512	Any value representing the number of files when LOG_FILE_DELETE_METHOD is 2. Any value representing the number of hours when LOG_FILE_DELETE_METHOD is assigned a value of 3. The value assigned should be greater than LOG_FILE_ROLL_METHOD_VALUE if LOG_FILE_ROLL_METHOD is assigned a value of 1.
LOG_CACHE_BUFFER_SIZE	80	Any value representing the size in KB. The value assigned should not exceed the available memory on the server.
DATE_TIME_FORMAT	2	1 = Do not insert a date and time stamp for each entry to the log file. 2 = Insert a date and time stamp for each entry to the log file. The date and time have the format of MM/DD/YYYY, HH:MM:SS +/- TimeZoneOffset, where MM is the month, DD is the day, and YYYY is the year.

If global logging for IP has been enabled, the Novell® BorderManager™ server is also configured by default to shut down the public interface when logging fails to occur. A logging failure can occur when the server experiences a shortage of disk space. If you want to disable the automatic shutdown of the public interface when logging fails, at the server console enter

SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = OFF

To reenable the automatic shutdown of the public interface, enter

SET SHUTDOWN PUBLIC INTERFACE ON LOG FAILURE = ON

Viewing IP Packet Log Information

The IP packet filter logs stored in the SYS:ETC\LOGS\IPPKTLOG directory can be viewed with any text editor. Because the log file conforms to the Microsoft* standard format, the data in the log file can be imported by most third-party applications for analysis.

Each entry in the log file contains the following fields:

- Date
- Time
- Source IP Address
- Destination IP Address
- Protocol
- Source Port
- Destination Port
- TCP Flags
- Access—1 indicates accept; 0 indicates deny
- IP Header
- IP Payload

Note A dash (-) appearing in any of the fields indicates that the information was unavailable or did not apply to the type of packet that was logged.