

# Compatible Systems Tech Notes: Searching the Log for Filtered Traffic

Document ID: 17667

---

- Introduction**
- Prerequisites**
  - Requirements
- Affected Products**
- Affected Versions**
- More Information**
- Related Information**

---

## Introduction

This document discusses how to search the device log to see what your filter or firewall blocks and how to let it through.

## Prerequisites

### Requirements

There are no specific requirements for this document.

## Affected Products

900i, 1200i, 1220i, 1250i, 1270i, 2600i, 2900i, 2200R, 2220R, 2250R, 2270R, 3500R, 3800R, 4000S, VSR-2 VSR-8, and IntraGuard

## Affected Versions

All versions

## More Information

Very often when you use a firewall or filter, you block some type of traffic that you would rather not be blocked. Knowing what ports or protocols to allow through is the key to getting this traffic through. In order to determine what is blocked, the easiest method is to refer to the device log.

If you use a filter, add the word **log** to the end of the filter line you suspect is blocking your good traffic. It looks something like this:

```
permit 0.0.0.0 0.0.0.0 tcp est
deny 0.0.0.0 0.0.0.0 log
```

\*\* Remember that the default last rule of any filter is to deny anything not specifically permitted in the filter. So even if we have a filter that says:

```
deny 0.0.0.0 0.0.0.0 tcp dst = 23
```

as the only line in our filter (thinking that it would deny telnet) it actually denies everything because it does not permit anything. It really looks like this:

```
deny 0.0.0.0 0.0.0.0 tcp dst = 23
deny 0.0.0.0 0.0.0.0
```

So after you add the "log" to the end of the deny all line, try to establish the connection that seems to be blocked by the filter. You then see that everything that "log" line denies now shows up in the log like this:

```
Notice 38.6 seconds IP FILTER: `test` rule# 1:
deny: src=198.41.9.61(2001) dst=204.144.171.12(23) proto=6
```

The port numbers are after the respective IP address that it is associated with. This line in the log shows that a telnet from port 2001 of 198.41.9.61 to destination of telnet port 23 on 204.144.171.12 was denied by filter rule #1 of filter test. So if you want to let this through you need to add a line to the "test" filter that says:

```
permit 198.41.9.61 204.144.171.12 tcp dst = 23
```

Ensure that this line is before the deny in the filter itself, or the traffic might be denied and thrown out before it ever reaches your new permit line. The order of the filter lines is very important because they are applied from top to bottom.

Look for the IP address of either the workstation you are attempting to make the connection with or the server you are trying to contact. This is the traffic that is blocked that you wish to allow through.

The IP protocols, other than IP itself, can be specified as a decimal number or as a keyword. The supported keywords are listed here by their protocol numbers for your reference.

```
TCP (6)
UDP (17)
ICMP (1)
GRE (47)
AH (51)
OSPF (89)
ESP (50)
```

Then you are able to determine what is blocked and what you need to let through.

Another good command from a telnet is the **show ip filter** command which shows how many matches each line of the filter had whether it permitted it through or denied it.

```
Test_Router#show ip filter
Filter Spec: test (1)
 1: deny 0.0.0.0/00000000 -> 0.0.0.0/00000000
    Protocol: ==TCP Dst == 23
    Options: LOG
    Matches: 4:
 2: permit 0.0.0.0/00000000 -> 0.0.0.0/00000000
    Protocol: ==IP
    Matches: 171:
```

The IntraGuard Firewall works in the same manner, but since the filters are built in, the IntraGuard automatically logs the failed attempts to the device log. Search through for the workstation and server and you can determine what is blocked. You can then either allow that port in or out for that firewall path, or apply an

OrFilterIn to allow that traffic in to your network. An OrFilterIn is created like a normal filter, but is used to permit certain traffic through the firewall on that path. You only need to permit that specific traffic that is blocked by the firewall and you do not need to worry about the deny all of a normal filter.

---

## Related Information

- [Technical Support & Documentation – Cisco Systems](#)
- 

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jun 20, 2007

Document ID: 17667

---