

# **HP-UX IPFilter A.03.05.14 Release Notes**

**HP-UX 11i v1 and  
HP-UX 11i v2**

**December 2006**

**Documentation Web Site: <http://www.docs.hp.com>**



**i n v e n t**

**Manufacturing Part Number : B9901-90032  
E1206**

United States

© Copyright 2001-2006 Hewlett-Packard Development Company, L.P.

---

## Legal Notices

The information contained herein is subject to change without notice.

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

### U.S. Government License

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

Copyright © 2001–2006 Hewlett-Packard Development Company, L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

### Trademark Notices

UNIX® is a registered trademark of The Open Group.

### Acknowledgements

This product includes software developed by Darren Reed and is based on IPFilter Version 3.5 Alpha 5. This documentation is based on information from the IPFilter How-To documentation, located at <http://caligula.anu.edu.au/~avalon>.

# 1 HP-UX IPFilter Release Notes

---

## Announcement

HP-UX IPFilter, product number B9901AA version A.03.05.14 is a TCP/IP packet filter suitable for use as a system firewall to protect application servers. The firewall functions as a security defense by cutting down the number of exposure points on a machine. Although HP-UX IPFilter is a superset of the functionality in the IPFilter 3.5 Alpha 5 open source version of the product (developed by Darren Reed), HP does not support some of the perimeter firewall features in that release.

For a complete list of commands and utilities that are not supported by HP, see “Unsupported Features” on page 7.

The HP-UX IPFilter version A.03.05.14 product is supported on HP-UX 11i v1 and HP-UX 11i v2 systems. The software includes all the functionality found in the open source code including the unsupported perimeter firewall features, such as firewall stealth (fastroute). If you are using features that are not supported by HP, you can request support from the open source IPFilter website. The URL for this site is <http://caligula.anu.edu.au/~avalon>.

HP-UX IPFilter A.03.05.14 can be obtained from the HP Software Depot at <http://www.software.hp.com> for HP-UX 11i v1 and HP-UX 11i v2. In addition, HP-UX IPFilter A.03.05.14 will be available on AR/OE media for HP-UX 11i v1 and HP-UX 11i v2 in 2007.

## What's in This Version

### Benefits and Features

HP-UX IPFilter version A.03.05.14 provides the following key benefits:

- Protects an individual host on an intranet against internal attacks
- Protects an individual host on an intranet against external attacks which have breached perimeter defenses
- Provides an alternative to the restricted configuration of Internet Services
- Protects bastion host on the perimeter or in the DMZ

The following major features are included with HP-UX IPFilter version A.03.05.14:

- Explicitly permits or denies a packet from passing through based on:
  - IP address or a range of IP addresses
  - IP protocol (IP/TCP/UDP)
  - IP fragments
  - IP options
  - IP security classes
  - TCP ports and port ranges
  - UDP ports and port ranges
  - ICMP message type and code
  - Combination of TCP flags
  - Interface
- Allows control of incoming TCP connections through DCA
- Supports NAT, which lets an intermediate HP-UX system act as a translator of IP addresses and network ports
- Sends back ICMP error/TCP reset for blocked packets
- Keeps packet state information for TCP, UDP, and ICMP
- Keeps fragment state information for any IP packet, applying the same rule to all fragments

- Drops all fragmented traffic if specified by rule
- Redirects packets for forensic analysis if specified by rule
- Creates extensive logs when required

HP-UX IPFilter version A.03.05.14 contains IPv6 support as described in “Enhancements” on page 14 of this Release Note.

## Known Problems and Workarounds

- The startup script for HP-UX IPFilter automatically disables the *ip\_forward\_directed\_broasts* parameter. This keeps the system from being subjected to broadcast-storm attacks that can bring down a network.

## Unsupported Features

The following list of utilities and commands are a part of the open source IPFilter product. These utilities and commands are included with HP-UX IPFilter, but are not supported by HP.

- Rule Keywords
  - fastroute
  - dropsafe logging keyword `dup-to`
  - dropsafe logging keyword `to`
- Commands
  - ipscan
  - ipsyns
  - ipsyncm
  - ipfs
  - ipsend
  - ipresend
  - mkfilters
  - auth
  - preauth
- Application proxy
- The `fr_limitmax` tunable has been deprecated and no longer used to control the number of limit entries that can be created on the system.

## **Features Not Supported with IPv6**

The following features are not supported with IPv6:

- Dynamic Connection Allocation (DCA) (the configuration of the IPv6 keep limit rules is not allowed.)
- IPFilter NAT functionality and the associated commands and utilities
- The `ipftest` utility
- RPC scripts
- IPFilter group rules

---

## Supported and Unsupported Interfaces

The following table lists the interfaces supported for each version of HP-UX IPFilter.

---

**CAUTION** For all versions of HP-UX IPFilter, the unsupported interfaces do not interact with IPFilter. IPFilter does not block or protect the system from traffic on unsupported interfaces.

---

HP-UX IPFilter is not tested with any third party products.

**Table 1-1 HP-UX IPFilter Supported Interfaces**

| HP-UX IPFilter Version                                                                    | Supported Interfaces                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.03.05.14<br>A.03.05.12<br>A.03.05.11.01<br>A.03.05.10<br>A.03.05.10.02<br>A.03.05.06.v2 | <ul style="list-style-type: none"><li>• Ethernet (10Base-T)</li><li>• Fast Ethernet (100Base-T)</li><li>• Gigabit Ethernet (1000Base-T)</li><li>• APA</li><li>• VLAN</li><li>• FDDI</li><li>• Token Ring</li><li>• InfiniBand (supported on HP-UX 11i v2 only)</li></ul> |
| A.03.05.10.04                                                                             | <ul style="list-style-type: none"><li>• Ethernet (10Base-T)</li><li>• Fast Ethernet (100Base-T)</li><li>• Gigabit Ethernet (1000Base-T)</li><li>• APA</li><li>• VLAN</li><li>• FDDI</li><li>• Token Ring</li></ul>                                                       |

**Table 1-1 HP-UX IPFilter Supported Interfaces (Continued)**

| <b>HP-UX IPFilter Version</b> | <b>Supported Interfaces</b>     |
|-------------------------------|---------------------------------|
| A.03.05.09                    | • Ethernet (10Base-T)           |
| A.03.05.08                    | • Fast Ethernet (100Base-T)     |
| A.03.05.07                    | • Gigabit Ethernet (1000Base-T) |
| A.03.05.06                    | • APA                           |
|                               | • VLAN                          |
|                               | • FDDI                          |
|                               | • Token Ring                    |

The following interfaces are unsupported (not protected by HP-UX IPFilter) on any HP-UX IPFilter releases:

- ATM
- Hyperfabric
- X.25
- Frame Relay
- PPP

## Compatibility Information and Installation Requirements

### Software Requirements

The system must have standard HP-UX 11i v1 or HP-UX 11i v2 core products installed on it. It must also have the following patches:

---

**NOTE** For HP-UX 11i v2, no patches are required, but it is recommended that you install the HP-UX 11i v2 December 2006 update.

---

- HP-UX 11i v1 Support Plus general release patch bundle (XSWGR1100)
- In addition, install the following required dependent patches for your system before you install HP-UX IPFilter:
  - HP-UX 11i v1 32-bit system  
PHCO\_22989 (or newer replacement) S700\_800 11.11 Som2elf patch
  - HP-UX 11i v1 64-bit system  
None
- HP recommends that DLKM users also add the following patches. These patches will make the DLKM subsystem more robust.
  - HP-UX 11i v1 32-bit system  
PHKL\_22994 (or newer replacement) S700\_800 11.11 fixes DLKM load unreg+text size panics
  - HP-UX 11i v1 64-bit system  
PHKL\_22994 (or newer replacement) S700\_800 11.11 fixes DLKM load unreg+text size panics
- If you are using HP-UX IPFilter IPv6 functionality, you must install TOUR 3.1.

## Compatibility Information and Installation Requirements

- If you are using HP-UX IPFilter with VLAN, you must install the following patches:
  - PHNE\_24491 Gigabit Ethernet
  - PHNE\_25388 LAN
  - PHNE\_23465 BTLAN
  - PHNE\_29887 ARPA/Transport

You can also add the following patches for additional functionality:

- PHCO\_24118 cumulative SAM/ObAM
- PHNE\_24473 *nettl* (1M), *netfmt* (1M), *nettladm* (1M)

You should install HP-UX IPFilter with `swinstall` (SD-UX) at any time after the system has been ignited with all other software and applied with all required patches. HP-UX IPFilter is a dynamically loadable kernel module (DLKM). It will be automatically registered with the running kernel during product installation.

## Hardware Requirements

HP 9000 workstations and servers and HP Integrity Systems

## OS Platform and Version Compatibility

HP-UX 11i v1 and HP-UX 11i v2

## Other Requirements

ICMPv6 filtering must be carefully configured to ensure that an IPv6 network functions properly. For example, do not block Neighbor Discovery messages (type 135 and 136). Other examples of critical ICMPv6 messages are Destination Unreachable (type 1) and Packet Too Big (type 2).

HP-UX IPFilter enables you to uniquely identify an ICMPv6 message using its type and code. A new keyword, `icmpv6-type`, is introduced. Use the following rule to pass ICMPv6 type 135 code 0 packets:

```
pass in quick proto icmpv6 from any to any icmpv6-type 135 code 0
```

---

**NOTE** The type and code can only be specified as a decimal number.

---

At minimum, the following rules must be configured:

```
pass in quick proto icmpv6 from any to any icmpv6-type 133
pass in quick proto icmpv6 from any to any icmpv6-type 134
pass in quick proto icmpv6 from any to any icmpv6-type 135
pass in quick proto icmpv6 from any to any icmpv6-type 136
pass out quick proto icmpv6 from any to any icmpv6-type 133
pass out quick proto icmpv6 from any to any icmpv6-type 134
pass out quick proto icmpv6 from any to any icmpv6-type 135
pass out quick proto icmpv6 from any to any icmpv6-type 136
```

The following is additional information about message types 133-136:

- 133—Router solicitation
- 134—Router advertisement
- 135—Neighbor solicitation
- 136—Neighbor advertisement

## Disk Space Required for Installation

This product requires 10 Mbytes of disk space.

## Common Mistakes or Gotchas

None

## Enhancements

### IPv6 Support

IPv6 support has been added to HP-UX IPFilter. The following IPv6 features are included:

- Provides IPv6 equivalent filtering for IPv6 while maintaining IPv4 support:
  - Filtering on IPv6 addresses, address-ranges, and prefixes
  - Filtering on ports and port ranges
  - Filtering on IPv6 physical interfaces
  - Filtering on ULP (TCP/UDP/ICMP)
  - Filtering using any combination of these
- Stateful Filtering for TCP (limited for UDP and ICMPv6)
- IPv6 fragmentation support (ability to block fragmented traffic)
- Filter on extension headers:
  - Filter packets with specific extension headers
- Filter on v6-in-v4 filtered traffic and v6-in-v6 traffic
- Detect IPSec headers (ah/esp) and pass if it matches a pass rule or block if it matches a block
- Provide IPv6 filter statistics
- Neighbor discovery (ICMPv6 rules to pass critical ICMPv6 messages)
- Recognize and filter on new ICMPv6 messages

For more information, see the *HP-UX IPFilter A.03.05.14 Administrator's Guide*.

## Fixes in This Version

### Fixes for HP-UX 11i v1 and HP-UX 11i v2

The following problems have been fixed in HP-UX IPFilter version A.03.05.14 for HP-UX 11i v1 and HP-UX 11i v2.

- JAGaf15610 (8606354854)—Cannot delete "head keyword rule" by `ipf -r -f` command.
- JAGaf53050 (8606392975)—There is a note that is not necessary in *ipf*(5) online manual.
- JAGaf92103 (8606432664)—When skip rule is set, the packet is blocked unspecified.
- JAGaf92106 (8606432667)—The way to increment pkts & bytes is illegal.
- JAGaf97189 (8606439188)—NAT rule is not effective upper 256 session.
- JAGag24098 (8606468829)—`pass return-rst` is accepted by `ipf` command.
- JAGag24099 (8606468830)—`ipf` accepts incorrect not rule.

## List of Documents Available with Product

The list below contains documentation related to the HP-UX IPFilter product.

- *HP-UX IPFilter A.03.05.14 Administrator's Guide* (B9901-90031)
- *HP-UX IPFilter A.03.05.14 Release Notes* (B9901-90032)

HP-UX IPFilter documentation is available from the following sources:

- The HP Technical Documentation Web Site at <http://docs.hp.com/en/internet.html>
- Instant Information documentation CD

For information about HP-UX Bastille, see the “HP-UX Bastille” section of *Managing Systems and Workgroups: A Guide for HP-UX System Administrators*. This guide is available at:

<http://docs.hp.com/hpux/os/11iv2/index.html#System%20Administration>