HP-UX IPFilter V18.21 Release Notes
HP-UX 11i v3

Abstract

This document provides information about new and changed features for HP-UX IPFilter V.18.21. This document is intended for anyone who installs and uses HP-UX IPFilter. The information in this document assumes that you have experience with administering an HP-UX operating system.

HP Part Number: 761996-002
Published: March 2015
Edition: 1

Legal Notices

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.

Contents

HP secure development lifecycle

Starting with HP-UX 11i v3 March 2013 update release, HP secure development lifecycle provides the ability to authenticate HP-UX software. Software delivered through this release has been digitally signed using HP's private key. You can now verify the authenticity of the software before installing the products, delivered through this release.

To verify the software signatures in signed depot, the following products must be installed on your system:

- `B.11.31.1303` or later version of SD (Software Distributor)
- `A.01.02.00` or later version of HP-UX Whitelisting `(WhiteListInf)`

To verify the signatures, run: `/usr/sbin/swsign -v -s <depot_path>`.

For more information, see *Software Distributor documentation* at http://www.hp.com/go/sd-docs.

NOTE: Ignite-UX software delivered with HP-UX 11i v3 March 2014 release or later supports verification of the software signatures in signed depot or media, during cold installation.

For more information, see *Ignite-UX documentation* at http://www.hp.com/go/ignite-ux-docs.

1 About this product

HP-UX IPFilter, product number B9901AA V18.21 is a TCP/IP packet filter suitable for use as a system firewall to protect back-end 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. 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.

The HP-UX IPFilter V18.21 product is supported on HP-UX 11i v3 systems. HP-UX IPFilter V18.21 can be obtained from the HP Software Depot at http://www.software.hp.com under the **Security and manageability** link.

OS Version	HP-UX IPFilter Version String
HP-UX 11i v3	A.11.31.18.21

For a complete list of commands and utilities that are not supported by HP, see Section (page 14).

NOTE: This document is for HP-UX IPFilter V.18.21 on HP-UX 11i v3. The *HP-UX IPFilter V17.05 Release Notes* for HP-UX 11i v2 is available at HP Support Center.

Benefits and features

HP-UX IPFilter V.18.21 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 V18.21:

- 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
- Supports IPv6
- Supports IPv4 address pools

2 Enhancements in this release

This chapter discusses the new features or enhancements provided in this release.

- Support for LARGE NAT feature in IPFilter—

  Enabling LARGE NAT allows fine tuning of IPFilter NAT HASH table sizes. Tuning the HASH table sizes may reduce the number of HASH collisions, which results in faster search in the HASH tables and increased throughput.

  The size of all the hash tables is 127 by default. The size can be tuned using `kctune` parameters.

- To reduce write lock delays during NAT operation, performance improvements are done.

3 Fixes in this release

This chapter discusses the defects fixed in this release.

QXCR1001197925	TCP `S` flags option is not handled correctly with RFC 3168
QXCR1001205042	RE: `pfil*_precheck` call pfil_hook_get twice in perf path
QXCR1001206555	Inconsistent logging for UDP packets in a specific IPFilter configuration
QXCR1001258699	`age` value in NAT rule does not work for `FIN-WAIT-1 => CLOSING` transition
QXCR1001275195	IPFilter: `nat-tag` string logged while NAT tag is not configured
QXCR1001321580	Example policy from Administration guide fails with: unknown port "65536"

4 Compatibility information and installation requirements

Software requirements

The system must have standard HP-UX 11i v3 core products installed.

The following (or superseding) patches are required if you are using HP-UX IPFilter with VLAN:

- 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 is 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 v3

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 10MB of disk space.

5 Issues and solutions

- Using the `pps` option with `keep state`

  The rate base filtering option `pps` is only applied to the first occurrence of the packet for which state gets stored. That is, after a state entry is added into the state table, rate based filtering does not apply.

  For example:

  ```
  pass in quick proto tcp from any to 10.2.2.2/32 port = 80 flags S keep state pps 10
  ```

  In the above example, rate based filtering is applied on the incoming connection (SYN packet) only. That is, not more than 10 TCP connections to 10.2.2.2 on port 80 are accepted per second. After the state table is created by SYN packets for those connections, the subsequent packets are not rate based filtered.

- The startup script for HP-UX IPFilter automatically disables the *`ip_forward_directed_broadcasts`* parameter. This keeps the system from being subjected to broadcast-storm attacks that can bring down a network.
- If rules are configured using stdin, rule numbers are not assigned properly to individual rules on entering **Ctrl-c** at the end. Sample output:

  ```
  # ipf -f-
  pass in on lan1 from 15.154.118.191/32 to 16.181.168.207/32
  pass in on lan1 from 15.154.118.192/32 to 16.181.168.207/32
  Ctrl-c

  # ipfstat -iohn
  empty list for ipfilter(out)
  0 @0:0 pass in on lan1 from 15.154.118.191/32 to 16.181.168.207/32
  0 @0:0 pass in on lan1 from 15.154.118.192/32 to 16.181.168.207/32
  ```

  To load the rules properly, enter end of file control character at the end of the rules. Sample output:

  ```
  # ipf -f-
  pass in on lan1 from 15.154.118.191/32 to 16.181.168.207/32
  pass in on lan1 from 15.154.118.192/32 to 16.181.168.207/32
  Ctrl-d

  # ipfstat -iohn
  empty list for ipfilter(out)
  0 @0:1 pass in on lan1 from 15.154.118.191/32 to 16.181.168.207/32
  0 @0:2 pass in on lan1 from 15.154.118.192/32 to 16.181.168.207/32
  ```

- `l4check` rules
  - `l4check` adds or deletes rules with only one IP address. RDR rules with only one IP address are ignored.
  - `l4check` does not have the option to add rules with sticky keyword.
- Excluding nodes in `ippool` using "!" does not work for hash type pools.

  ```
  # cat ippool.conf
  table role = ipf type = hash number = 10
         {192.168.1.1/24; ! 192.168.1.88/32;};
  #ippool -f ippool.conf
  syntax error error at "!", line 2
  ```

6 Other product information

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 HP-UX IPFilter supported interfaces

IPFilter version	Supported interfaces
A.11.31.18.0 A.11.31.18.10	• Ethernet (10Base-T) • Fast Ethernet (100Base-T)

Table 1 HP-UX IPFilter supported interfaces *(continued)*

IPFilter version	Supported interfaces
A.11.31.18.21	• Gigabit Ethernet (1000Base-T) • 10 Gigabit Ethernet • APA • VLAN • FDDI • Token Ring • X.25 (supported on HP-UX 11i v3 only)
A.11.xx.17.xx	• Ethernet (10Base-T) • Fast Ethernet (100Base-T) • Gigabit Ethernet (1000Base-T) • 10 Gigabit Ethernet • APA • VLAN • FDDI • Token Ring • InfiniBand (supported on HP-UX 11i v2 only) • X.25 (supported on HP-UX 11i v3 only)
A.11.xx.16	• Ethernet (10Base-T) • Fast Ethernet (100Base-T) • Gigabit Ethernet (1000Base-T) • 10 Gigabit Ethernet • APA • VLAN • FDDI • Token Ring • InfiniBand (supported on HP-UX 11i v2 only) • X.25 (supported on HP-UX 11i v3 only)
A.11.xx.15.01	• Ethernet (10Base-T) • Fast Ethernet (100Base-T) • Gigabit Ethernet (1000Base-T) • APA • VLAN • FDDI • Token Ring • InfiniBand (supported on HP-UX 11i v2 only) • X.25 (supported on HP-UX 11i v3 only)
Open source versions: A.03.05.14 (HP-UX 11i v1 and HP-UX 11i v2) A.03.05.13 (HP-UX 11i v3) A.03.05.12 A.03.05.11.01 A.03.05.10	• Ethernet (10Base-T) • Fast Ethernet (100Base-T) • Gigabit Ethernet (1000Base-T) • APA • VLAN • FDDI

Table 1 HP-UX IPFilter supported interfaces *(continued)*

IPFilter version	Supported interfaces
A.03.05.10.02 A.03.05.10.04 A.03.05.06.v2	• Token Ring • InfiniBand (supported on HP-UX 11i v2 only)
Open source versions: A.03.05.09 A.03.05.08 A.03.05.07 A.03.05.06	• Ethernet (10Base-T) • Fast Ethernet (100Base-T) • Gigabit Ethernet (1000Base-T) • APA • VLAN • FDDI • Token Ring

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

- ATM
- Hyperfabric
- Frame Relay
- PPP

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`
  - `ipsyncs`
  - `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.
- The `ipfstat` command does not support authorization statistics.

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

7 Support and other resources

Contacting HP

Before you contact HP

Be sure to have the following information available before you contact HP:

- Technical support registration number (if applicable)
- Product serial number
- Product identification number
- Applicable error message
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

HP contact information

For the name of the nearest HP authorized reseller, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website: http://www.hp.com/go/hpsc.
- In other locations, see the Contact HP worldwide (in English) webpage: http://welcome.hp.com/country/us/en/wwcontact.html.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/country/us/en/contact_us.html

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related Information

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

- The HP Technical Documentation web Site at:

  http://www.hp.com/go/hpux-security-docs
- The Instant Information documentation CD

For more information on Configuring and Using HP-UX IPFilter, see *HP-UX IPFilter Version 18.21 Administrator Guide* at HP Support Center.

For information about HP-UX Bastille, see the *HP-UX Bastille Version User Guide* at:

HP Support Center.

Typographic conventions

This document uses the following typographical conventions:

`%`, `$`, or `#`	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells. A number sign represents the superuser prompt.
audit(5)	A manpage. The manpage name is *audit*, and it is located in Section 5.
`Command`	A command name or qualified command phrase.
`Computer output`	Text displayed by the computer.
Ctrl+x	A key sequence. A sequence such as **Ctrl+x** indicates that you must hold down the key labeled **Ctrl** while you press another key or mouse button.
`ENVIRONMENT VARIABLE`	The name of an environment variable, for example, `PATH`.
ERROR NAME	The name of an error, usually returned in the `errno` variable.
Key	The name of a keyboard key. **Return** and **Enter** both refer to the same key.
Term	The defined use of an important word or phrase.
`User input`	Commands and other text that you type.
`Variable`	The name of a placeholder in a command, function, or other syntax display that you replace with an actual value.
[]	The contents are optional in syntax. If the contents are a list separated by `|`, you must choose one of the items.
{}	The contents are required in syntax. If the contents are a list separated by `|`, you must choose one of the items.
...	The preceding element can be repeated an arbitrary number of times.
⌷	Indicates the continuation of a code example.
|	Separates items in a list of choices.
WARNING	A warning calls attention to important information that if not understood or followed will result in personal injury or nonrecoverable system problems.
CAUTION	A caution calls attention to important information that if not understood or followed will result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	This alert provides essential information to explain a concept or to complete a task.
NOTE	A note contains additional information to emphasize or supplement important points of the main text.

8 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Support policy for HP-UX

For more information about support policy for HP-UX, see HP-UX support policy.