

HP A-F1000-A-EI_A-F1000-S-EI VPN Firewalls

Attack Protection

Command Reference

Part number: 5998-2660

Document version: 6PW100-20110909



Legal and notice information

© Copyright 2011 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

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.

Contents

ARP attack protection configuration commands	1
Gratuitous ARP configuration commands	1
arp send-gratuitous-arp	1
gratuitous-arp-sending enable	2
gratuitous-arp-learning enable	2
ARP automatic scanning and fixed ARP configuration commands	3
arp fixup	3
arp scan	4
TCP attack protection configuration commands	5
display tcp status	5
tcp anti-naptha enable	6
tcp state	6
tcp syn-cookie enable	7
tcp timer check-state	8
Firewall configuration commands	9
display firewall ipv6 statistics	9
firewall ipv6 default	10
firewall ipv6 enable	11
firewall packet-filter ipv6	11
reset firewall ipv6 statistics	12
Support and other resources	13
Contacting HP	13
Subscription service	13
Related information	13
Documents	13
Websites	13
Conventions	14
Index	15

ARP attack protection configuration commands

Gratuitous ARP configuration commands

arp send-gratuitous-arp

Syntax

arp send-gratuitous-arp [**interval** *milliseconds*]

undo arp send-gratuitous-arp

View

Layer 3 Ethernet interface view, Layer 3 Ethernet subinterface view, Layer 3 aggregate interface view, Layer 3 aggregate subinterface view, VLAN interface view

Default level

2: System level

Parameters

interval *milliseconds*: Sets the interval at which gratuitous ARP packets are sent, in the range of 200 to 200000 milliseconds. The default value is 2000.

Description

Use the **arp send-gratuitous-arp** command to enable periodic sending of gratuitous ARP packets and set the sending interval for the interface.

Use the **undo arp send-gratuitous-arp** command to disable the interface from periodically sending gratuitous ARP packets.

By default, an interface is disabled from sending gratuitous ARP packets periodically.

Note that:

- This function takes effect only when the link of the enabled interface goes up and an IP address has been assigned to the interface.
- The IP address contained in a gratuitous ARP request can be the VRRP virtual IP address, the primary IP address or a manually configured secondary IP address of the sending interface only. The primary IP address can be configured manually or automatically, whereas the secondary IP address must be configured manually.
- If you change the interval for sending gratuitous ARP packets, the configuration is effective at the next sending interval.
- The frequency of sending gratuitous ARP packets may be much lower than is expected if this function is enabled on multiple interfaces, or each interface is configured with multiple secondary IP addresses, or a small sending interval is configured in the preceding cases.

Examples

```
# Enable GigabitEthernet 0/1 to send gratuitous ARP packets every 300 milliseconds.
```

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 0/1
```

```
[Sysname-GigabitEthernet0/1] arp send-gratuitous-arp interval 300
```

gratuitous-arp-sending enable

Syntax

```
gratuitous-arp-sending enable  
undo gratuitous-arp-sending enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use the **gratuitous-arp-sending enable** command to enable the firewall to send gratuitous ARP packets when receiving ARP requests from another network segment.

Use the **undo gratuitous-arp-sending enable** command to restore the default.

By default, the firewall cannot send gratuitous ARP packets when receiving ARP requests from another network segment.

Examples

```
# Disable the firewall from sending gratuitous ARP packets.  
<Sysname> system-view  
[Sysname] undo gratuitous-arp-sending enable
```

gratuitous-arp-learning enable

Syntax

```
gratuitous-arp-learning enable  
undo gratuitous-arp-learning enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function.

Use the **undo gratuitous-arp-learning enable** command to disable the function.

By default, the function is enabled.

With this function enabled, the firewall receiving a gratuitous ARP packet can add the source IP and MAC addresses to its own dynamic ARP table if it finds no ARP entry in the cache corresponding to the source IP address of the ARP packet exists. If a matching ARP entry is found in the cache, the firewall updates the ARP entry regardless of whether this function is enabled.

Examples

```
# Enable the gratuitous ARP packet learning function.  
<Sysname> system-view  
[Sysname] gratuitous-arp-learning enable
```

ARP automatic scanning and fixed ARP configuration commands

arp fixup

Syntax

arp fixup

View

System view

Default level

2: System level

Parameters

None

Description

Use the **arp fixup** command to change the existing dynamic ARP entries into static ARP entries. You can use this command again to change the dynamic ARP entries learned later into static.

Note the following:

- The static ARP entries changed from dynamic ARP entries have the same attributes as the manually configured static ARP entries.
- The number of static ARP entries changed from dynamic ARP entries is restricted by the number of static ARP entries that the device supports. As a result, the device may fail to change all dynamic ARP entries into static ARP entries.
- Suppose that the number of dynamic ARP entries is D and that of the existing static ARP entries is S . When the dynamic ARP entries are changed into static, new dynamic ARP entries may be created (suppose the number is M) and some of the dynamic ARP entries may be aged out (suppose the number is N). After the process is complete, the number of static ARP entries is $D + S + M - N$.
- To delete a specific static ARP entry changed from a dynamic one, use the **undo arp ip-address [vpn-instance-name]** command. To delete all such static ARP entries, use the **reset arp all** or **reset arp static** command.

Examples

```
# Enable Fixed ARP.  
<Sysname> system-view
```

```
[Sysname] arp fixup
```

arp scan

Syntax

```
arp scan [ start-ip-address to end-ip-address ]
```

View

Layer 3 Ethernet interface view, Layer 3 Ethernet subinterface view, Layer 3 aggregate interface view, Layer 3 aggregate sub-interface view

Default level

2: System level

Parameters

start-ip-address: Start IP address of the scanning range.

end-ip-address: End IP address of the scanning range. The end IP address must be higher than or equal to the start IP address.

Description

Use the **arp scan** command to enable ARP automatic scanning in the specified address range for neighbors.

Note the following:

- If the start IP and end IP addresses are specified, the device scans the specific address range for neighbors and learns their ARP entries, so that the scanning time is reduced. If the specified address range contains multiple network segments, the sender IP address in the ARP request is the interface address on the smallest network segment.
- If no address range is specified, the device only scans the network where the primary IP address of the interface resides for neighbors. The sender IP address in the ARP requests is the primary IP address of the interface.
- The start IP address and end IP address must be on the same network as the primary IP address or manually configured secondary IP addresses of the interface.
- IP addresses already exist in ARP entries are not scanned.
- ARP automatic scanning may take some time. To stop an ongoing scan, press **Ctrl + C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.

Examples

Configure the device to scan the network where the primary IP address of GigabitEthernet 0/1 resides for neighbors.

```
<Sysname> system-view  
[Sysname] interface GigabitEthernet 0/1  
[Sysname-GigabitEthernet0/1] arp scan
```

Configure the device to scan the specific address range for neighbors.

```
<Sysname> system-view  
[Sysname] interface GigabitEthernet 0/1  
[Sysname-GigabitEthernet0/1] arp scan 1.1.1.1 to 1.1.1.20
```

TCP attack protection configuration commands

display tcp status

Syntax

```
display tcp status [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Getting Started Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display tcp status** command to display status of all TCP connections for monitoring TCP connections.

Examples

```
# Display status of all TCP connections.
```

```
<Sysname> display tcp status
```

```
*: TCP MD5 Connection
```

```
TCPCB          Local Add:port      Foreign Add:port     State
03e37dc4       0.0.0.0:4001        0.0.0.0:0           Listening
04217174       100.0.0.204:23     100.0.0.253:65508   Established
```

Table 1 Output description

Field	Description
*: TCP MD5 Connection	If the status information of a TCP connection contains *, the TCP adopts the MD5 algorithm for authentication.
TCPCB	TCP control block
Local Add:port	Local IP address and port number
Foreign Add:port	Remote IP address and port number
State	State of the TCP connection

tcp anti-naptha enable

Syntax

```
tcp anti-naptha enable
undo tcp anti-naptha enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use the **tcp anti-naptha enable** command to enable the protection against Naptha attack.

Use the **undo tcp anti-naptha enable** command to disable the protection against Naptha attack.

By default, the protection against Naptha attack is disabled.

The configurations made by using the **tcp state** and **tcp timer check-state** commands will be removed after the protection against Naptha attack is disabled.

Examples

```
# Enable the protection against Naptha attack.
<Sysname> system-view
[Sysname] tcp anti-naptha enable
```

tcp state

Syntax

```
tcp state { closing | established | fin-wait-1 | fin-wait-2 | last-ack | syn-received } connection-number
number
undo tcp state { closing | established | fin-wait-1 | fin-wait-2 | last-ack | syn-received }
connection-number
```

View

System view

Default level

2: System level

Parameters

closing: CLOSING state of a TCP connection.

established: ESTABLISHED state of a TCP connection.

fin-wait-1: FIN_WAIT_1 state of a TCP connection.

fin-wait-2: FIN_WAIT_2 state of a TCP connection.

last-ack: LAST_ACK state of a TCP connection.

syn-received: SYN_RECEIVED state of a TCP connection.

connection-number *number*: Maximum number of TCP connections in a certain state. The argument *number* is in the range of 0 to 500.

Description

Use the **tcp state** command to configure the maximum number of TCP connections in a state. When this number is exceeded, the aging of TCP connections in this state will be accelerated.

Use the **undo tcp state** command to restore the default.

By default, the maximum number of TCP connections in each state is 5.

Note the following points:

- You need to enable the protection against Naptha attack before executing this command. Otherwise, an error will be prompted.
- You can respectively configure the maximum number of TCP connections in each state.
- If the maximum number of TCP connections in a state is 0, the aging of TCP connections in this state will not be accelerated.

Related commands: **tcp anti-naptha enable**.

Examples

```
# Set the maximum number of TCP connections in the ESTABLISHED state to 100.
<Sysname> system-view
[Sysname] tcp anti-naptha enable
[Sysname] tcp state established connection-number 100
```

tcp syn-cookie enable

Syntax

tcp syn-cookie enable

undo tcp syn-cookie enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **tcp syn-cookie enable** command to enable the SYN Cookie feature to protect the device against SYN Flood attacks.

Use the **undo tcp syn-cookie enable** command to disable the SYN Cookie feature.

By default, the SYN Cookie feature is enabled.

Examples

```
# Enable the SYN Cookie feature.
<Sysname> system-view
```

```
[Sysname] tcp syn-cookie enable
```

tcp timer check-state

Syntax

```
tcp timer check-state time-value
```

```
undo tcp timer check-state
```

View

System view

Default level

2: System level

Parameters

time-value: TCP connection state check interval in seconds, in the range of 1 to 60.

Description

Use the **tcp timer check-state** command to configure the TCP connection state check interval.

Use the **undo tcp timer check-state** command to restore the default.

By default, the TCP connection state check interval is 30 seconds.

The device periodically checks the number of TCP connections in each state. If it detects that the number of TCP connections in a state exceeds the maximum number, it will accelerate the aging of TCP connections in such a state.

Note that you need to enable the protection against Naptha attack before executing this command. Otherwise, an error will be prompted.

Related commands: **tcp anti-naptha enable**.

Example

```
# Set the TCP connection state check interval to 40 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] tcp anti-naptha enable
```

```
[Sysname] tcp timer check-state 40
```

Firewall configuration commands

display firewall ipv6 statistics

Syntax

```
display firewall ipv6 statistics { all | interface interface-type interface-number } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the packet filtering statistics of all interfaces of the IPv6 firewall.

interface *interface-type interface-number*: Displays the packet filtering statistics of the specified interface of the IPv6 firewall.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Getting Started Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display firewall ipv6 statistics** command to view the packet filtering statistics of the IPv6 firewall.

Examples

Display the packet filtering statistics of the IPv6 firewall.

```
<Sysname> display firewall ipv6 statistics interface GigabitEthernet 0/1
  Interface: GigabitEthernet0/1
  In-bound Policy: acl6 2000
  From 2008-06-04 10:25:21 to 2008-06-04 10:35:57
    0 packets, 0 bytes, 0% permitted
    0 packets, 0 bytes, 0% denied
    0 packets, 0 bytes, 0% permitted default
    0 packets, 0 bytes, 0% denied default
  Totally 0 packets, 0 bytes, 0% permitted
  Totally 0 packets, 0 bytes, 0% denied
```

Table 2 Output description

Field	Description
Interface	Interface configured with the IPv6 packet filtering function
In-bound Policy	Indicates that an IPv6 ACL is configured in the inbound direction of the interface
Out-bound Policy	Indicates that an IPv6 ACL is configured in the outbound direction of the interface
acl6	IPv6 ACL number
0 packets, 0 bytes, 0% permitted	Indicates the packets permitted by IPv6 ACL rules: the number of packets and bytes, and the percentage of the permitted to the total.
0 packets, 0 bytes, 0% denied	Indicates the packets denied by IPv6 ACL rules: the number of packets and bytes, and the percentage of the denied to the total.
0 packets, 0 bytes, 0% permitted default	Indicates the packets that matched no IPv6 ACL rule and were permitted according to the default filtering rule: number of packets and bytes, and the percentage of the permitted to the total.
0 packets, 0 bytes, 0% denied default	Indicates the packets that matched no IPv6 ACL rule and were denied according to the default filtering rule: number of packets and bytes, and the percentage of the denied to the total.
Totally 0 packets, 0 bytes, 0% permitted	Indicates all permitted packets: the number of packets and bytes, and the percentage of all the permitted to the total.
Totally 0 packets, 0 bytes, 0% denied	Indicates all denied packets: the number of packets and bytes, and the percentage of all the denied to the total.

firewall ipv6 default

Syntax

```
firewall ipv6 default { deny | permit }
```

View

System view

Default level

2: System level

Parameters

deny: Specifies the filtering action as denying packets to pass the firewall.

permit: Specifies the filtering action as permitting packets to pass the firewall.

Description

Use the **firewall ipv6 default** command to specify the default firewall filtering action of the IPv6 firewall.

By default, the default filtering action of IPv6 firewall is permitting packets to pass (**permit**).

Examples

```
# Specify the default filtering action of the IPv6 firewall as denying packets to pass.
<Sysname> system-view
[Sysname] firewall ipv6 default deny
```

firewall ipv6 enable

Syntax

```
firewall ipv6 enable
undo firewall ipv6 enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use the **firewall ipv6 enable** command to enable the IPv6 firewall function.

Use the **undo firewall ipv6 enable** command to disable the IPv6 firewall function.

By default, the IPv6 firewall function is disabled.

Examples

```
# Enable the IPv6 firewall function.
<Sysname> system-view
[Sysname] firewall ipv6 enable
```

firewall packet-filter ipv6

Syntax

```
firewall packet-filter ipv6 { acl6-number | name acl6-name } { inbound | outbound }
undo firewall packet-filter ipv6 [ { acl6-number | name acl6-name } ] { inbound | outbound }
```

View

Interface view

Default level

2: System level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999; advanced ACL number, in the range of 3000 to 3999.

name *acl6-name*: Specifies the name of a basic or advanced IPv6 ACL; a case-insensitive string of 1 to 32 characters that must start with an English letter a to z or A to Z. To avoid confusion, the word “all” cannot be used as the ACL name.

inbound: Specifies to filter packets received by the interface.

outbound: Specifies to filter packets forwarded by the interface.

Description

Use the **firewall packet-filter ipv6** command to configure IPv6 packet filtering on the interface.

Use the **undo firewall packet-filter ipv6** command to remove the IPv6 packet filtering setting on the interface.

By default, IPv6 packets are not filtered on the interface.

Examples

```
# Configure IPv6 packet filtering for GigabitEthernet 0/1 using IPv6 ACL 2500.
```

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 0/1
```

```
[Sysname-GigabitEthernet0/1] firewall packet-filter ipv6 2500 outbound
```

reset firewall ipv6 statistics

Syntax

```
reset firewall ipv6 statistics { all | interface interface-type interface-number }
```

View

User view

Default level

1: Monitor level

Parameters

all: Clears the packet filtering statistics on all interfaces of the IPv6 firewall.

interface *interface-type interface-number*: Clears the packet filtering statistics on the specified interface of the IPv6 firewall.

Description

Use the **reset firewall ipv6 statistics** command to clear the packet filtering statistics of the IPv6 firewall.

Related commands: **display firewall ipv6 statistics**.

Examples

```
# Clear the packet filtering statistics on GigabitEthernet 0/1 of the IPv6 firewall.
```

```
<Sysname> reset firewall ipv6 statistics interface GigabitEthernet 0/1
```

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

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

<http://www.hp.com/go/wwalerts>

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

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP A-Series Acronyms*.

Websites

- HP.com <http://www.hp.com>
- HP Networking <http://www.hp.com/go/networking>
- HP manuals <http://www.hp.com/support/manuals>
- HP download drivers and software <http://www.hp.com/support/downloads>
- HP software depot <http://www.software.hp.com>

Conventions

This section describes the conventions used in this documentation set.





Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x y ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x y ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x y ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x y ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
 TIP	An alert that provides helpful information.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

A D E G R S T W

A

- arp fixup, [3](#)
- arp scan, [4](#)
- arp send-gratuitous-arp, [1](#)

D

- display firewall ipv6 statistics, [9](#)
- display tcp status, [5](#)
- Documents, [13](#)

F

- firewall ipv6 default, [10](#)
- firewall ipv6 enable, [11](#)
- firewall packet-filter ipv6, [11](#)

G

- gratuitous-arp-learning enable, [2](#)
- gratuitous-arp-sending enable, [2](#)

R

- reset firewall ipv6 statistics, [12](#)

S

- Subscription service, [13](#)

T

- tcp anti-naptha enable, [6](#)
- tcp state, [6](#)
- tcp syn-cookie enable, [7](#)
- tcp timer check-state, [8](#)

W

- Websites, [13](#)