



Cisco ASR 5000 Series Personal Stateful Firewall Administration Guide - Errata

Release 11.0 and 12.0

Last Updated April 30, 2012

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Personal Stateful Firewall Administration Guide - Errata

© 2012 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide V

 Conventions Usedvi

 Contacting Customer Supportviii

 Additional Informationix

Affected Document(s)..... 11

Sample Personal Stateful Firewall Configuration 13

About this Guide





This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5x00 Chassis.

This preface includes the following sections:

- [Conventions Used](#)
- [Contacting Customer Support](#)
- [Additional Information](#)

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a <i>screen display</i>	This typeface represents text that appears on your terminal screen, for example: <i>Login:</i>
Text represented as commands	This typeface represents commands that you enter at the CLI, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are <u>not</u> case sensitive.
Text represented as a command variable	This typeface represents a variable that is part of a command, for example: show card slot_number <i>slot_number</i> is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New .

Command Syntax Conventions	Description
{ keyword or <i>variable</i> }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[keyword or <i>variable</i>]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
	<p>Some commands support alternative variables. These “options” are documented within braces or brackets by separating each variable with a vertical bar.</p> <p>These variables can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>{ nonce timestamp }</pre> <p>OR</p> <pre>[count <i>number_of_packets</i> size <i>number_of_bytes</i>]</pre>

Contacting Customer Support

Go to <http://www.cisco.com/cisco/web/support/> to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

Refer to the following guides for supplemental information about the system:

- *Command Line Interface Reference*
- *Statistics and Counters Reference*
- *Thresholding Configuration Guide*
- *SNMP MIB Reference*
- *Cisco Web Element Manager Installation and Administration Guide*
- Product-specific and feature-specific administration guides
- *Release Notes* that accompany updates and upgrades to StarOS

Chapter 1

Affected Document(s)

This errata provides corrections to any documentation errors in the *Personal Stateful Firewall Administration Guide* specific to Release 11.0 and 12.0 on the Cisco ASR 5000.

Documentation corrections provided in this errata pertain to the documents listed in the following table and correspond to the stated release dates:

Document	Part Number	Release Date
<i>Cisco ASR 5000 Personal Stateful Firewall Administration Guide: Version 11.0</i>	OL-24220-01	January 14, 2011
<i>Cisco ASR 5000 Personal Stateful Firewall Administration Guide: Version 12.0</i>	OL-24894-01	April 30, 2011

Chapter 2

Sample Personal Stateful Firewall Configuration

In the *Sample Personal Stateful Firewall Configuration* chapter of the affected books, the “**tcp packets-out-of-order timeout**” and “**tcp packets-out-of-order transmit after-reordering**” commands are not applicable to Stateful Firewall functionality. The commands are specific to Active Charging Service functionality. The following is the correct sample configuration.

```
configure

  license key "\

VER=1|C1M=SanDiskSDJNJKL742749406|C1S=14J3KJI20|DOI=108|DOE=12\

SIG=MC4CFQCf9f7bAibGKJWqMd5XowxVwIVALIVgTVDsVAAogKe7fUHAEUTokw"

  aaa default-domain subscriber radius

  aaa last-resort context subscriber radius

  gtp single-source

  system hostname ABCCH4

  autoconfirm

  clock timezone asia-calcutta

  crash enable encrypted url 123abc456def789ghi

  card 1

    mode active psc

    exit

  card 2

    mode active psc

    exit

  card 4

    mode active psc

    exit

  require session recovery
```

```
require active-charging

context local

    interface SPI01

        ip address 1.2.3.4 255.255.255.0

        exit

    server ftpd

        exit

    ssh key 123abc456def789ghi123abc456def789ghi len 461

    server sshd

        subsystem sftp

        exit

    server telnetd

        exit

    subscriber default

        exit

    administrator staradmin encrypted password 123abc456def789ghi ftp

    aaa group default

        exit

    gtp group default

        exit

    ip route 0.0.0.0 0.0.0.0 2.3.4.5 SPI01

    exit

port ethernet 24/1

    no shutdown

    bind interface SPI01 local

    exit

ntp

    enable

    server 10.6.1.1
```

```
exit

snmp engine-id local 77777e66666a55555

active-charging service service_1

nat allocation-failure send-icmp-dest-unreachable

host-pool host1

    ip range 1.2.3.4 to 2.3.4.5

    exit

host-pool host2

    ip range 3.4.5.6 to 4.5.6.7

    exit

host-pool host3

    ip range 5.6.7.8 to 6.7.8.9

    exit

ruledef ip_any

    ip any-match = TRUE

    exit

ruledef rt_ftp

    tcp dst-port = 21

    rule-application routing

    exit

ruledef rt_ftp_data

    tcp dst-port = 20

    rule-application routing

    exit

ruledef rt_rtsp

    tcp dst-port = 554

    rule-application routing

    exit

ruledef rt_http
```

```
    tcp dst-port = 80

    rule-application routing
exit

ruledef rt_pptp

    tcp dst-port = 1723

    rule-application routing
exit

ruledef rt_tftp

    udp dst-port = 69

    rule-application routing
exit

access-ruledef fw_icmp

    icmp any-match = TRUE

    exit

access-ruledef fw_tcp

    tcp any-match = TRUE

    exit

access-ruledef fw_udp

    udp any-match = TRUE

    exit

edr-format nbr_format1

    attribute sn-start-time format MM/DD/YYYY-HH:MM:SS priority 5

    attribute sn-end-time format MM/DD/YYYY-HH:MM:SS priority 10

    attribute radius-nas-ip-address priority 15

    attribute sn-correlation-id priority 20

    rule-variable ip subscriber-ip-address priority 25

    rule-variable ip server-ip-address priority 30

    attribute sn-subscriber-port priority 35

    attribute sn-server-port priority 40
```



```
attribute sn-flow-id priority 45

attribute sn-volume-amt ip bytes uplink priority 50
attribute sn-volume-amt ip bytes downlink priority 55
attribute sn-volume-amt ip pkts uplink priority 60
attribute sn-volume-amt ip pkts downlink priority 65
attribute sn-volume-amt tcp pkts downlink priority 66
attribute sn-volume-amt tcp pkts uplink priority 67
attribute sn-volume-amt tcp bytes downlink priority 68
attribute sn-volume-amt tcp bytes uplink priority 69

rule-variable ip protocol priority 70
attribute sn-app-protocol priority 75
attribute radius-user-name priority 80
attribute radius-calling-station-id priority 85
attribute sn-direction priority 90

attribute sn-volume-dropped-amt ip bytes uplink priority 100
attribute sn-volume-dropped-amt ip bytes downlink priority 110
attribute sn-volume-dropped-amt ip packets uplink priority 115
attribute sn-volume-dropped-amt ip packets downlink priority 120
attribute sn-volume-dropped-amt tcp bytes uplink priority 130
attribute sn-volume-dropped-amt tcp bytes downlink priority 140
attribute sn-volume-dropped-amt tcp packets uplink priority 155
attribute sn-volume-dropped-amt tcp packets downlink priority 160

exit

udr-format udr_format

attribute sn-start-time format MM/DD/YYYY-HH:MM:SS localtime priority 1
attribute sn-end-time format MM/DD/YYYY-HH:MM:SS localtime priority 2
attribute sn-correlation-id priority 4
attribute sn-content-vol bytes uplink priority 6
attribute sn-content-vol bytes downlink priority 7
```

```
attribute sn-fa-correlation-id priority 8
attribute radius-fa-nas-ip-address priority 9
attribute radius-fa-nas-identifier priority 10
attribute radius-user-name priority 11
attribute sn-content-vol pkts uplink priority 12
attribute sn-content-vol pkts downlink priority 13
attribute sn-group-id priority 14
attribute sn-content-id priority 15
exit
xheader-format header
insert Stpid-1 variable bearer sn-rulebase
insert Stpid-2 variable bearer subscriber-ip-address
exit
charging-action ca_nothing
content-id 20
exit
bandwidth-policy bw1
exit
bandwidth-policy bw2
exit
rulebase base_1
route priority 1 ruledef rt_ftp analyzer ftp-control
route priority 10 ruledef rt_ftp_data analyzer ftp-data
route priority 20 ruledef rt_rtsp analyzer rtsp
route priority 40 ruledef rt_http analyzer http
route priority 50 ruledef rt_pptp analyzer pptp
route priority 60 ruledef rt_tftp analyzer tftp
rtp dynamic-flow-detection
fw-and-nat default-policy base_1
```

```
exit

rulebase base_2

    action priority 1 ruledef ip_any charging-action ca_nothing

    route priority 1 ruledef rt_ftp analyzer ftp-control

    route priority 10 ruledef rt_ftp_data analyzer ftp-data

    route priority 40 ruledef rt_http analyzer http

    route priority 50 ruledef rt_pptp analyzer pptp

    route priority 60 ruledef rt_tftp analyzer tftp

    bandwidth default-policy bw2

    fw-and-nat default-policy base_2

exit

rulebase default

    exit

fw-and-nat policy base_1

    access-rule priority 1 access-ruledef fw_tcp permit

    access-rule priority 2 access-ruledef fw_udp permit

    firewall dos-protection source-router

    firewall dos-protection winnuke

    firewall dos-protection mime-flood

    firewall dos-protection ftp-bounce

    firewall dos-protection ip-unaligned-timestamp

    firewall dos-protection tcp-window-containment

    firewall dos-protection teardrop

    firewall dos-protection flooding udp

    firewall dos-protection flooding icmp

    firewall dos-protection flooding tcp-syn

    firewall dos-protection port-scan

    firewall dos-protection ipv6-dst-options invalid-options

    firewall dos-protection ipv6-extension-hdrs limit 2
```

■ Additional Information

```
firewall dos-protection ipv6-hop-by-hop jumbo-payload

firewall dos-protection ipv6-hop-by-hop router-alert

firewall tcp-first-packet-non-syn reset

firewall policy ipv4-and-ipv6

exit

fw-and-nat policy base_2

    access-rule priority 5 access-ruledf fw_tcp_port_3000 permit trigger open-port
5000 direction reverse

    access-rule priority 10 access-ruledf fw_tcp permit

    access-rule priority 20 access-ruledf fw_udp permit

    access-rule priority 30 access-ruledf fw_icmp deny

    firewall policy ipv4-and-ipv6

    exit

nat tcp-2msl-timeout 120

exit

context pdsn

    interface pdsn

        ip address 11.22.33.44 255.255.255.0

        ip address 22.33.44.55 255.255.255.0 secondary

        exit

ssh key 123abc456def789ghi123abc456def789ghi len 461

server sshd

    subsystem sftp

    exit

subscriber default

    ip access-group css-1 in

    ip access-group css-1 out

    ip context-name isp

    mobile-ip send accounting-correlation-info
```

```
        active-charging rulebase base_1

    exit

aaa group default

    exit

gtpv group default

    exit

pdsn-service pdsn

    spi remote-address 1.1.1.1 spi-number 256 encrypted secret 5c4a38dc2ff61f72
timestamp-tolerance 0

    spi remote-address 2.2.2.2 spi-number 256 encrypted secret 5c4a38dc2ff61f72
timestamp-tolerance 0

    spi remote-address 3.3.3.3 spi-number 9999 encrypted secret 5c4a38dc2ff61f72
timestamp-tolerance 0

    authentication pap 1 chap 2 allow-noauth

    bind address 4.4.4.4

    exit

edr-module active-charging-service

    file name NBR_nat current-prefix Record rotation time 45 headers edr-format-name

    exit

exit

context isp

    ip access-list css

        redirect css service service_1    ip any any

        exit

    ip pool pool1 5.5.5.5 255.255.0.0 public 0

    interface isp

        ip address 6.6.6.6 255.255.255.0

        exit

    subscriber default

    exit
```

■ Additional Information

```
aaa group default
    exit

gtpv group default
    exit

ip route 0.0.0.0 0.0.0.0 7.7.7.7 isp

exit

context radius

interface radius

    ip address 8.8.8.8 255.255.255.0

    exit

subscriber default

    exit

subscriber name ABC7-sub

    ip access-group css in

    ip access-group css out

    ip context-name isp

    active-charging rulebase base_1

    exit

subscriber name ABC9-sub

    ip access-group css in

    ip access-group css out

    ip context-name ispl

    active-charging rulebase base_2

    exit

domain ABC7.com default subscriber ABC7-sub

domain ABC9.com default subscriber ABC9-sub

radius change-authorize-nas-ip 77.77.77.77 encrypted key 123abc456def789ghi port
4000

aaa group default
```

```

radius attribute nas-ip-address address 99.99.99.99

radius dictionary custom9

radius server 9.9.9.9 encrypted key 123abc456def789gh port 1645

radius accounting server 8.8.8.8 encrypted key 123abc port 1646

exit

gtp group default

exit

diameter endpoint acs-fire.star.com

    origin host acs-fire.star.com address 44.44.44.44

    peer minid realm star.com address 55.55.55.55

exit

exit

bulkstats collection

bulkstats mode

    sample-interval 1

    transfer-interval 15

    file 1

        remotefile format /localdisk/ABCCH4.bulkstat

        receiver 66.66.66.66 primary mechanism ftp login root encrypted password
123abc456def789ghi

        context schema sfw-dir format "sfw-dir\nsfw-dnlk-dropkts:%sfw-dnlk-
dropkts%\nsfw-dnlk-dropbytes:%sfw-dnlk-dropbytes%\nsfw-uplnk-dropkts:%sfw-uplnk-
dropkts%\nsfw-uplnk-dropbytes:%sfw-uplnk-dropbytes%\nsfw-ip-discardpackets:%sfw-ip-
discardpackets%\nsfw-ip-malpackets:%sfw-ip-malpackets%\nsfw-icmp-discardpackets:%sfw-
icmp-discardpackets%\nsfw-icmp-malpackets:%sfw-icmp-malpackets%\nsfw-tcp-
discardpackets:%sfw-tcp-discardpackets%\nsfw-tcp-malpackets:%sfw-tcp-malpackets%\nsfw-
udp-discardpackets:%sfw-udp-discardpackets%\nsfw-udp-malpackets:%sfw-udp-malpackets%\n---
-----\n"

        context schema sfw-total format "sfw-
total\nvpname:%vpname%\nvpnid:%vpnid%\nsfw-total-rxpackets:%sfw-total-rxpackets%\nsfw-
total-rxbytes:%sfw-total-rxbytes%\nsfw-total-txpackets:%sfw-total-txpackets%\nsfw-total-
txbytes:%sfw-total-txbytes%\nsfw-total-injectedpkts:%sfw-total-injectedpkts%\nsfw-total-
injectedbytes:%sfw-total-injectedbytes%sfw-total-malpackets:%sfw-total-malpackets%\nsfw-
total-dosattacks:%sfw-total-dosattacks%\nsfw-total-flows:%sfw-total-flows%\n-----
-----\n"

```

■ Additional Information

```
        exit
    exit
port ethernet 17/1
    no shutdown
    bind interface pdsn pdsn
    exit
port ethernet 17/2
    no shutdown
    bind interface isp isp
    exit
port ethernet 17/3
    no shutdown
    bind interface radius radius
    exit
port ethernet 17/4
    no shutdown
    exit
port ethernet 17/5
    no shutdown
    exit
end
```