If you want to make sure that the firewall accepted the flags, you need to run : *fw ctl debug –m rtm*

Flag	Explanation
chain	displays information about chain registering, and about the E2E chain function actions; this important flag helps you know if the E2E (VL) is identifying VL packets.
driver	displays general driver information (loading / unloading, etc).
error	different error messages (default)
import	displays information about RTM importing functions from other modules (FW-1, FG-1)
init	*rarely used*
ioctl	RTM IOCTL printouts
kviews	Kernel Views debugging (when you open / close a GUI or CLI client)
netmasks	displays information about how the RTM handles netmasks, if you are monitoring network object, which is a network
per_conn	messages per connection (when a new connection is handled by RTM)
per_pckt	messages per packet (when a new packet arrives) - use it with care
policy	displays FireWall-1 load/unload messages (indicates that the RTM received the FW-1 callback)
rtm	displays information about RTM monitoring
rtmpkt	displays per packet information while RTM is monitoring (generates a large amount of output)
sort	debugging the RTM top X monitoring sorting
sort_start	display sorting statistics (used to debug algorithm efficiency)
special	display information about how E2E modifies E2ECP protocol packets
topo	display information about how the RTM calculates network topography
view_add	when Views are added or deleted
view_update	when Views are updated with new information
view_update1	when Views are updated with new information

Kernel debugging options for InterSPECT module: interspect

If you want to make sure that the firewall accepted the flags, you need to run : fw ctl debug –m interspect + *flag*

Flag	Explanation
dynlog	dynamic logging
mail	mail security in the kernel
portscan	port scanning issues
sam	SAM IP blocking

Kernel debugging options for Streams module: strmod
Solution ID: #10043.0.9927750.2843527 (Activating streams module debugging) - *Internal*

If you want to make sure that the firewall accepted the flags, you need to run : *fw ctl debug –m strmod*

Flag	Explanation
errack	error ACK from data link
filter	streams module filter (such as fastpath)
fpack	ACK from data link on fastpath
fpnak	No ACK from data link on fastpath
if	interface and Qdata information (see sk17136)
iferr	problems with interface Qdata
ipctl	IP control commands
ipmsg	*currently unused*
msg	messages in the stream queues
msgerr	problems with handling messages from stream queues
oftab	oftabs information (oftabs hold interface data)
ofterr	problems with oftabs
okack	OK ACK from data link
open	opening or closing devices/queues
openerr	problems opening or closing devices / queues
state	state of the Data-Link attachment

If you want to make sure that the firewall accepted the flags, you need to run : *fw ctl debug –m cluster*

Note:
- There is also the SYNC flag, which is in the FW topic and shows debug that is related to SYNC only.
- To get a better debug in case you have a failover issue, please set the following kernel parameters to 1:
  fw ctl set int fwha_dprint_io 1
  fw ctl set int fwha_dprint_all_net_check 1

Flag	Explanation
accel	accelerator messages
ccp	Cluster Control Protocol (CCP)
conf	configuration-related messages
df	Decision Function - decides, which member will handle each packet in a Load Sharing mode
drop	connections dropped by the CXL Decision Function (DF) module (only in **NGX**)
forward	Forwarding Layer messages - when sending and receiving a forwarded packet
if	interface tracking and validation - all the operations and checks on interfaces
log	logging
mac	MAC address synchronization
nokia	relevant for cluster running on IPSO platform
pivot	relevant for ClusterXL Load Sharing Unicast mode (Pivot mode)
pnote	pnote device related (a general mechanism for registering and monitoring critical devices)
select	packet selection - including Decision Function (DF)
stat	ClusterXL state machine
subs	monitoring of the new cxl_status_api module reports and changes; this module is a set of APIs, which enable user space processes (by using a DLL) to be aware of the current state of the ClusterXL state machine and also other clustering configuration parameters.
timer	reports of timer ticks (pours many messages, without real content)

Kernel debugging options for Web Intelligence module: WS

If you want to make sure that the firewall accepted the flags, you need to run : *fw ctl debug –m WS*

Flag	Explanation
address	IP address information connection
body	HTTP body (content) layer
connection	connection layer
coverage	function coverage
error	errors: the connection is probably rejected
fatal	fatal errors: may prevent policy installation, etc.
global	global structure handling (usually policy related)
info	informational purposes only
ioctl	IOCTLs - policy (installation) related
mem_pool	memory pool related
memory	memory allocation issues - memory leak and error detection
module	module related
parser	HTTP header parser layer
pfinder	pattern finder related
pkt_dump	traffic packet dump (requires connection)
policy	policy (installation) related
regexp	regular expression library
report_mgr	report manager (errors and logs)
session	session layer
spii	INSPECT streaming - SPII related
sslt	SSLT library
sslt_seq	SSLT sequence library
stat	memory usage statistics
subject	shows the debug subject of each message
timestamp	a timestamp for each debug message (changes when 'coverage' is active)
uuid	session UUID related
warning	warnings: may affect connection behavior

fw ctl set ip ws_debug_ip <IP_address> = debug of a specific IP
fw ctl set ip ws_debug_ip 0 = stops debug of a specific IP

If you want to make sure that the firewall accepted the flags, you need to run : *fw ctl debug –m fw*

Flag	Explanation
align	*currently unused* - H.323 (VoIP)
balance	logical servers in kernel , load balancing
bridge	*currently unused*
chain	cookie chain , chain modules
chainfwd	chain forwarding - related to fwha_perform_chain_forwarding global kernel variable
cifs	Common Internet File System (CIFS) - file sharing protocol in Windows-based networks
citrix	Citrix processing
conn	connection table issues
content	AV content inspection
cookie	virtual de-fragmentation , cookie issues
cprx	regular expressions mechanics - old engine
crypt	encryption issues
domain	domain resolution issues , DNS enforcement
driver	kernel attachment
drop	associates a reason for (almost) every dropped packet
dynlog	dynamic log enhancement (inspect logs)
error	default output
ex	table expiration issues (time-out)
filter	policy installation , SAM , fw monitor , boot-time policy
hold	packets hold mechanics
if	network interface tracking and validation - all the operations and checks on interfaces
install	network interface attachment (fw ctl install and uninstall)
integrity	client integrity mechanics
ioctl	IOCTLs - policy (installation) related
ipopt	IP options enforcement
kbuf	kernel buffers
ld	kernel dynamic tables infrastructure (very useful, but loads CPU – the machine can hang)
leaks	memory leak detection mechanism
link	connection table link creation
log	logging
machine	Virtual Machine operations
mail	e-mail issues - POP3, IMAP
media	ARP, non-IP packets
memory	memory allocation issues - memory leak and error detection
mgcp	Media Gateway Control Protocol (complementary to H.323 and SIP)
misc	miscellaneous issues (especially licensing), sqlnet, internal name resolution, CSV
misp	ISP Redundancy
msnms	MSN over MSMS (MSN Messenger protocol) - always include sip flag
nat	NAT issues - basic operation
packet	virtual de-fragmentation ; actions on packets, especially KFUNCs called by INSPECT
packval	stateless verifications - sequences, fragments, translations and other header verifications
portscan	port scanning prevention mechanics
q	synchronization operations – crucial for cluster debugging ; message queues
route	Routing debugging (ISP Redundancy, fwcookie code)
sam	Suspicious Activity Monitoring
scv	SecureClient Verification
sip	SIP (VoIP)
smtp	e-mail issues
spii	Stateful Protocol Inspection Infrastructure (INSPECT streaming) (only in **NGX**)
synatk	SYNDefender
sync	synchronization operations in cluster
tcpstr	TCP streaming mechanism
vm	virtual machine chain decisions on traffic going through `fw filter chain` (only in **NGX**)
wap	Multimedia Messaging Service (Wireless Application Protocol)
warning	warnings may be suppressed, but are still printed by default (except on SR / SC)
wire	wire-mode Virtual Machine chain module
xlate	NAT issues - including dynamic NAT
xltrc	NAT issues - complex services (such as FTP)