Firewall Services Module and PIX Commands

This appendix describes additions, changes, and differences between the Firewall Services Module and the PIX application commands.

The tables in this appendix describe the following commands:

- Commands that support the maintenance software (Table A-1 on page A-1).
- Cisco IOS commands that support the Firewall Services Module (Table A-2 on page A-3).
- Catalyst operating system commands that support the Firewall Services Module (Table A-3 on page A-3).
- New commands specific to the module (Table A-4 on page A-3).

  These commands are described in Appendix B, "Command Reference."
- PIX commands that were changed for the module (Table A-5 on page A-5).
- PIX commands that are not used by the module (Table A-6 on page A-5).
- PIX commands used by the module and their PIX version (Table A-7 on page A-7).

  For detailed information about the PIX software commands, refer to the PIX documentation listed in the "Related Documentation" section on page xvii.

The module also supports CLI commands for the supervisor engine, which are described in more detail in the *Catalyst 6500 Series Command Reference*.

Table A-1 Administrative Commands Supporting the Maintenance Software

Command	Description
clear ip	Clears the network configuration for the interface.
clear log upgrade	Clears the application image upgrade log file. This command is available only in the maintenance image.
clear password	Clears and resets the password.
disable-guest	Disables the guest account from the maintenance image. This command is available only for the root account. The guest account is enabled by default.
enable-guest	Enables the guest account from the maintenance image root account. This command is available only for the root account. The guest account is enabled by default.

Table A-1 Administrative Commands Supporting the Maintenance Software (continued)

Command	Description
?	Displays a list of top-level commands or additional information for an individual command.
ip	Sets the IP parameters. This command is available from the application and maintenance image and the guest account in the maintenance image.
ip address *ip-address netmask*	Specifies the IP address and subnet for a node on the network.
ip broadcast *broadcast-address*	Specifies the IP broadcast address for a node on the network.
ip domain *domain-name*	Specifies the domain name.
ip gateway *gateway-address*	Specifies the default IP gateway.
ip host *hostname*	Specifies an IP host name.
ip nameserver [*name-server1*] [*name-server2*] [*name-server3*]	Specifies the IP name server used to resolve network names into network addresses.
logout	Logs you out of the shell from the maintenance image and the guest account from the maintenance image.
passwd	Sets the password for the current user from the root account.
passwd-guest	Sets the password for the guest account from the maintenance image. This command is available only for the root account.
ping *hostname* | *IP address*	Sends five ICMP echo-request packets to another node on the network. To configure ping, you can also use the command without arguments.
show	Displays the system parameters from the maintenance and guest account from the maintenance image.
show images	Lists the images that are installed in the module application partitions.
show ip	Displays current IP configuration.
show log upgrade	Displays the application image upgrade log.
show version	Displays the module maintenance image version, daughter card information, and module application image version.
show crashdump	Displays the contents of the crashdump partition. The partition is populated when the module application software crashes.
upgrade [*ftp-url*] [*device:partition-num*]	Upgrades the maintenance image from the specified location, when the module is booted into the application image. This command is also available from the guest account in the maintenance image.

Table A-2 Cisco IOS Commands for the Firewall Services Module

Command	Description
firewall module *module_number* **vlan-group** *firewall_group*	Attaches the VLAN and firewall group to the slot where the module is located.
firewall vlan-group *firewall_group vlan_range*	Creates a firewall group of controlled VLANs.
interface vlan *vlan_number*	Defines a controlled VLAN (SVI) on the MSFC (route processor). **Note** You must configure a controlled VLAN (SVI) on the MSFC or you will be unable to configure VLANs on the module.
show firewall module	Displays the module configuration.
show firewall vlan-group	Displays the firewall VLAN group.
show interface vlan *vlan_number*	Displays the interface configuration.
show firewall module	Displays the module configuration.
vlan *vlan_number*	Creates VLANs on the switch.

Table A-3 Catalyst Operating System Commands for the Firewall Services Module

Command	Descriptions
set vlan *vlan-range* **firewall-vlan** *module*	Sets the specified VLAN range as secure VLANs on the firewall module.
clear vlan *vlan-range* **firewall-vlan** *module*	Clears the specified VLANs from the secure VLANs for a given firewall module.
show vlan firewall-vlan *module*	Displays the current secure VLANs for a given firewall module.

Table A-4 New Firewall Services Module Commands

Command
access-list *id* **deny** | **permit** {**any** | *ip mask*}
area *area id* **authentication areadefault-cost** **area** *area id* **authentication message-digest** **area** *area id cost* **area** *area id* **filter-list prefix** *module* [**in** | **out**] **area** *area id* **nssa** [**no-redistribution**] [**default-information-originate**] **area** *area id* **range** *prefix mask* [**advertise** | **not-advertise**] **area** *area id stub* [**no-summary**] **area** *area id* **virtual-link** *router id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [t**ransmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*]| [**message-digest-key** *key id* **md5** *key*]]
console-output (clear and show)
default-information originate [**metric** *value* | **metric-type** { **1** | **2** } | **route-map** *map*]
distance [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]

Table A-4 New Firewall Services Module Commands (continued)

Command
ip prefix-list *list-module* [**seq** *seq-value*] {**deny** | **permit network/length**}[**ge** *ge-value*] [**le** le-value]
ip prefix-list *sequence-number*
logging rate-limit *num* [*interval*] **message** *syslog_id* **logging rate-limit** *num* [*interval*] **level** *syslog_level* **show logging rate-limit** **clear logging rate-limit**
match [**interface** | **route-type** | **metric** | **ip address** | **ip next-hop** | **ip route-source**]
moduleif *vlan_id* [**if_module**] [**security_level**]
network *prefix mask* **area** *area id*
ospf cost *cost* **ospf retransmit-interval** *seconds* **ospf transmit-delay** *seconds* **ospf priority** *number* **ospf hello-interval** *seconds* **ospf dead-interval** *seconds* **ospf authentication-key** *key* **ospf message-digest-key** *keyed* **md5** *key* **ospf authentication** [**message-digest** | **null**]
redistribute { *ospf* **id** | **static** | **connect** } [{**match** { **internal** | **external** *extern-type* } **metric** *metric-value* | **metric-type** *metric-type* [**internal** | **external**] **tag** *tag-value* | **subnets** }] **route-map** *map value*
route-map *map-tag* [**permit** | **deny**] [*seq-num*]
router ospf *asystem id*
set metric [**+** | **-**] *metric-value* **set metric-type type-1** | **type-2** | **internal** | **external** **set ip next-hop** *ip-addres*> [*ip-address...*]
show ip ospf **show ip ospf border-routers** **show ip ospf database** [**router**][**network**][**external**] **show ip ospf interface** **show ip ospf neighbor** **show ip ospf request-list** **show ip ospf retransmission-list** **show ip ospf summary-addres**s **show ip ospf virtual-link**
summary-address *addr mask* [**not-advertise**] [**tag** *tag*]
timers lsa-group-pacing *value* ***timers spf***
upgrade-mp

Table A-5 PIX Commands Changed for the Firewall Services Module

Command
aaa authentication [supervisor | enable | telnet | ssh | http] console *group_tag*
fragment size *database-limit* [*interface*] The default fragment size was changed from 200 for PIX to1 for the FWSM. By default, fragmentation is disabled on the FWSM.
icmp permit | deny [**host**] *src_addr* [*src_mask*] [*type*] *int_name* By default, ICMP is set to off in the FWSM.
interface *hardware_id* [**hardware_speed**] [**shutdown**] **show interface**
nameif *hardware_id ifname security_level* New syntax is **nameif** *vlan_id if_name security_level*. Refer to nameif vlan_number if_name security_level in Appendix B, "Command Reference"
route *if_module ip_address netmask gateway_ip* [*metric*]

Table A-6 PIX Commands Not Used by the Firewall Services Module

Command
apply [(if_name)] list_ID outgoing_src | outgoing_dest **clear apply** **show apply [(if_name)] [list_ID outgoing_src | outgoing_dest]**
failover rsa key
clock set hh:mm:ss month day year **clock set hh:mm:ss day month year** **show clock**
conduit permit | deny protocol *global_ip global_mask* [**operator port** [**port**]] *foreign_ip foreign_mask* [**operator port** [**port**]]
configure floppy
dhcpd auto_config [**client_ifx_name**] **dhcpd option** {**150 | 66**}
eeprom update **show eeprom**
flashfs downgrade {**4.x | 5.0 | 5.1**}
filter activex port *local_ip mask foreign_ip mask* **filter java port** [*-port*] *local_ip mask foreign_ip mask*
ip address *if_name* **dhcp** [**setroute**]

Table A-6 PIX Commands Not Used by the Firewall Services Module (continued)

Command
ip audit attack [**action** [**alarm**] [**drop**] [**reset**]] **show ip audit attack**
ip audit info [**action** [**alarm**] [**drop**] [**reset**]] **show ip audit info**
ip audit interface *if_module audit_module* **show ip audit interface**
ip audit name *audit_name* **attack** [**action** [**alarm**] [**drop**] [**reset**]] **show ip audit name** [**module** [**info** | **attack**]]
ip audit name *audit_name* **info** [**action** [**alarm**] [**drop**] [**reset**]] **show ip audit name**
ip audit module *audit_module* **info** [**action** [**alarm**] [**drop**] [**reset**]] **show ip audit module**
ip audit signature *signature_number* **disable** **show ip audit signature** [*signature_number*] **clear ip audit** [**module** | **signature** | **interface** | **attack** | **info**]
outbound *list_ID* **permit** | **deny** *ip_address* [*netmask* [**port**[-*port*]] [*protocol*] **outbound** *list_ID* **except** *ip_address* [*netmask* [**port**[-*port*]] [*protocol*] **clear outboun**d **show outbound**
session enable **show session**
sysopt uauth allow-http-cache **sysopt connection permit-pptp** **sysopt connection permit-l2tp**
vpdn enable *if_name* **vpdn group module accept dialin pptp** | **l2tp** **vpdn group module l2tp tunnel hello** *hello_timeout* **vpdn group** *group_module* **ppp authentication pap** | **chap** | **mschap** **vpdn group group_module ppp encryption mppe 40** | **128** | **auto** [**required**] **vpdn group** *group_module* **client configuration address local** *address_pool_module* **vpdn group** *group_module* **client configuration dns** *dns_server_ip1* [*dns_server_ip2*] **vpdn group** *group_module* **client configuration wins** *wins_server_ip1* [*wins_server_ip2*] **vpdn group** *group_module* **client authentication aaa** *aaa_server_group* **vpdn group** *group_module* **client authentication local** **vpdn group** *group_module* **client accounting** *aaa_server_group* **vpdn usermodule** *usermodule* password *password* **vpdn group** *group_module* **pptp echo** *echo_timeout* **show vpdn tunnel** [**l2tp** | **pptp**] [**id** *tunnel_id* | **packets** | **state** | **summary** | **transport**] **show vpdn usermodule** [**usermodule**] **show vpdn session** [**l2tp** | **pptp**] [**id** *session_id* | **packets** | **state** | **window**] **show vpdn pppinterface** [**id** *intf_id*] **clear vpdn** [**group** | **usermodule** | **tunnel** [**all** | [**id** *tunnel_id*]]]
write floppy

Table A-7 lists the PIX commands used by the module and their PIX version. Commands that were changed from PIX for the module are described in Appendix B, "Command Reference." For detailed information about the PIX software commands, refer to the PIX documentation located at these URLs:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/

Table A-7 PIX Commands and Versions

Command	PIX Version
aaa	6.0
aaa proxy-limit	6.2
aaa-server	6.0
access-group	6.0
arp	6.0
auth-prompt	6.0
ca-authorization	6.2
ca generate rsa key	6.0
clear console-output, page B-12	6.0
clear logging rate-limit, page B-13	6.0
default-information originate, page B-14	6.0
clear pager, page B-15	6.0
configure	6.0
console-output	6.0
copy tftp flash	6.0
nameif, page B-23	6.0
debug	6.0
dhcpd	6.0
disable	6.0
distance, page B-15	6.0
enable	6.0
enable password	6.0
established	6.0
exit	6.0
failover	6.2
failover lan interface	6.0
failover unit	6.0
filter	6.0
firewall module, page B-16	6.0
firewall vlan-group, page B-17	6.0
fixup protocol	6.2

Table A-7 PIX Commands and Versions (continued)

Command	PIX Version
floodguard	6.0
fragment	6.0
global	6.0
help	6.0
hostname	6.0
http	6.0
icmp	6.0
interface, page B-18	6.0
ip address	6.0
ip local pool	6.0
isakmp policy	6.0
kill	6.0
local-host (clear and show)	6.0
logging	6.0
logging rate-limit, page B-20	6.0
mtu	6.0
nameif, page B-23	6.0
name/ names	6.0
nat	6.0
object-group	6.2
pager	6.0
passwd	6.0
pdm	6.0
perfmon	6.0
ping	6.0
quit	6.0
reload	6.0
rip	6.0
route, page B-28	6.0
service	6.0
show	6.0
show apply	6.0
show blocks/ clear blocks	6.0
show checksum	6.0
show conn	6.0
show console-output, page B-35	6.0

Table A-7 PIX Commands and Versions (continued)

Command	PIX Version
show crashdump, page B-36	6.0
show firewall module, page B-37	6.0
show firewall vlan-group, page B-38	6.0
show history	6.0
show interface, page B-39	6.0
show logging rate-limit, page B-42	6.0
show memory	6.0
show pager	6.0
show processes	6.0
show sprom	6.0
show tech-support	6.0
show uauth	6.0
show version	6.0
show xlate	6.0
shun	6.0
snmp-server	6.0
ssh	6.0
static	6.0
syslog	6.0
sysopt	6.0
telnet	6.0
terminal	6.0
tftp-server	6.0
timeout	6.0
uauth (clear and show)	6.0
url-cache	6.2
url-server	6.0
virtual	6.0
who	6.0
write	6.0
xlate (clear and show)	6.0