The following table lists the differences among FWSM and ASA software configuration commands.

Feature/Command	**FWSM Description**	**ASA Description**
Connection timeouts for all protocols **set connection timeout idle**	The **idle** keyword was introduced in FWSM release 3.2(1). This command closes idle connections of all protocols after the specified period of time.	The **idle** keyword is not supported in ASA software. The ASA software has the **tcp** keyword, which is used to close TCP connections after a specified time.
Connection rate limit **set connection conn-rate-limit**	This command was introduced in FWSM release 4.0(1). It allows users to rate limit TCP and/or UDP connections to a value specified in the CLI.	This command is not present in ASA software.
AAA authentication challenge **aaa authentication challenge disable**	This command was introduced in FWSM release 3.1(1). This command disables authentication challenge for ftp, telnet, http, and https.	This command is not supported in ASA software.
AAA authentication clear conn **aaa authentication clear-conn**	This command was introduced in FWSM release 3.2(1). This command forces active connections to close immediately after user authentication times out or when the authentication session is cleared with the **clear uauth** command.	This command is not supported in ASA software.
Virtual SSH [no] **virtual ssh**	This command was introduced in FWSM release 3.2(1). This command allows direct authentication using SSH.	This command is not supported in ASA software.
Interactive password prompts with RADIUS for authentication **auth-prompt reject** [**invalid-credentials** | **expired-pwd**]	This command was introduced in FWSM release 1.1. The **invalid-credentials** and **expired-pwd** options were added in FWSM release 3.2(1). This command, with the new options, allows users to specify the strings during authentication rejection sdue to invalid credentials or expired passwords.	This command is supported in ASA software, but the **invalid-credentials** and **expired-pwd** options are not supported.
DHCP relay trusted interface (option 82) **dhcprelay information trusted dhcprelay information trust-all**	This command was introduced in FWSM command 4.0. This command allows users to preserve option 82 and forward a packet by identifying an interface as a trusted interface, ensuring that DHCP snooping and IP source guard features on the switch work along with the FWSM. The **trust-all** keyword enables the command for interfaces, as opposed to the **trusted** keyword, which enables the command for a single interface.	This command is not supported in ASA software.
http-map **port-misuse**	The command was introduced in FWSM release 3.1(1). This command restricts HTTP traffic by specifying a restricted application category. The **port-misuse** command is used in http map configuration mode, that is accessible using the **http-map** command.	This command is not supported in ASA software.

logging deny conn-queue-full	This command was introduced in FWSM release 3.1(1). When traffic is so heavy that the logging queue fills up, the FWSM might discard messages. This command prevents the creation of new transit connections through the FWSM to avoid discarding messages.	This command is not supported in ASA software.
CPU Threshold [no] **cpu threshold rising**	This command was introduced in FWSM release 3.2(1). When SNMP is enabled, traps are sent when the CPU levels reach a certain configurable mark.	This command is not supported in ASA software.
EtherType Access Lists and denying IPv4 and ARPs	In TFW mode with an ethertype access list configured to "deny all," both IPv4 and ARP cannot be denied on a FWSM device.	In TFW mode with an ethertype access list configured to "deny all," all ethertypes are denied, including IPv4 and ARP.
Direct Login or Logout using Virtual HTTP for User Authentication **virtual http ip_address** [**host** *hostname*]	Direct authentication including login and logout are supported using the **virtual http** command.	ASA software supports the login aspect of direct authentication but not logout. Because logout is not supported, direct authentication is not supported. ASA software does support cascading authentication with the **virtual http** command.
Route Monitoring **route-monitor**	The route-monitoring feature is supported. If multiple static routes are configured, the feature can detect if a network goes down and the next best route is used.	This feature is supported in ASA software using the **sla monitor** command. In this feature the ASA software supports more commmand options than FWSM software.
Old maps for inspections [no] **ftp-map** [no] **gtppmap** [no] **h225-map** [no] **http-map** [no] **mgcp-map** [no] **sip-map** [no] **snmp-map**	FWSM software still supports the old style xxx-map commands.	ASA software converted to the new style **policy-map'** ***and*** **policy-match** commands in release 7.2.
RIP **rip**	FWSM software still supports the old style single line **rip** configuration command.	ASA software converted to the new style multiline **rip** configuration command in

		release 7.2
TCP normalizer knob [no] **control-point tcp-normalizer**	FWSM software supports a limited TCP normalizer. This feature can be turned on or off using a knob.	ASA software does not have a knob to turn off the TCP normalizer.
Rate limits **access-list-commit** **allocate-acl-partition** **size** [no] **resource acl-partition** [no] **resource partition** [no] **resource rule** **rule**	Due to Hard NPs, FWSM has fixed rule limits and many commands to handle the limits.	ASA software does not have fixed rate limits, so it does not have these commands.
Xlates for all traffic [no] **xlate-bypass**	FWSM software always creates xlates for all traffic, including to-the-box traffic. This command was introduced to work around the xlate creation.	ASA software does not create xlates for all traffic, so it does not have these commands.
ACL optimization [no] **access-list optimization enable**	This command enables the access list optimization rules, which are optimized and downloaded to the Hard NPs. The command also reduces the number of ACEs for for each group.	This command is not supported in ASA software.
sysopt uauth allow-http-cache	This command is related to the direct authentication part of the **virtual http** command. When an authentication session times out and when a user connects again without this command, the user is prompted again for a username and password. If this command is used, then the web browser is allowed to supply the username and password from its cache.	This command is not present in ASA software.
sysopt np completion-unit	This command was introduced in FWSM release 3.2(5). This command allows users to enable the hardware completion unit in the accelerated path network processors (NPs), which ensures that packets are forwarded out in the same order in which they were received in the ingress queues of the NPs.	This command is not present in ASA software.
sysopt connection tcp sack-permitted	This command was introduced in FWSM release 3.1(12). The **no** form of the command allows users to clear the **sack permitted** option exchanged during the TCP three-way handshake. The **sack** option is enabled by	This command is implemented using the **tcp-options selective-ack clear / allow** command under tcp-map. The default is to

	default.	allow the **sack** option, as done in FWSM.
sysopt connection tcp window-scale	This command was introduced in FWSM release 3.1. Thi **no** form of the command allows users to clear the window-scale TCP option. The option is allowed by default.	This command is implemented using the **tcp-options window-scale** {**clear / allow**} command under tcp-map. The default is to allow the window-scale option, as done in FWSM.
Disaster Recovery **boot device module** *slot string*	This is a SUP command that allows for disaster recovery of FWSM software by specifying different compact flash partitions.	In ASA software disaster recovery is performed using ROMMOM and a console connection.
SNMP trap commands **snmp-server enable traps cpu threshold** **snmp-server enable traps cpu threshold rising** **snmp-server enable traps entity redun-switchover** **snmp-server enable traps entity alarm-asserted** **snmp-server enable traps entity alarm-cleared** **snmp-server enable traps nat** **snmp-server enable traps nat packet-discard** **snmp-server enable traps rate-limit-reached** **snmp-server enable traps resource** **snmp-server enable traps resource limit-reached**	These commands and the related traps were introduced in FWSM release 3.2(1).	These commands and the related traps are not supported in ASA software.
Service Reset [no] **service reset no-connection**	This command was introduced in FWSM release 4.0. This command configures the FWSM to send a RST for a TCP packet, for which the FWSM does not have any connection history.	ASA software achieves the same behavior using the **service resetinbound** command.
[no] **aaa schedule round-robin**	This command has no documentation, although it appears to have been introduced	This command is not present in ASA software.

	in FWSM release 3.1 to resolve an AAA bug, which states the following: "The problem is, we see a lot of stale https connections on the groupq, which is not allowing the other connections like telnet and ftp to pass though. This will result in a latency in echoing back the characters typed on the telnet client. To get away from this problem, we are creating a CLI **aaa schedule round-robin** which will schedule the groupq and allow other connections to be processed smoothly, if there are any stale https connections. Use the no form of this command to make the groupq to be processed in FIFO format (which is the default)."	
Resource limits **limit-resource ipsec** *value / value%* **limit-resource mac-addresses** *value / value%* **limit-resource rate fixups** *value* **limit-resource rate** *resource value%*	The **limit resource** command supports rate limit % as the resources have upper limits. It also supports limiting MAC addresses and IPSec management tunnels.	ASA software does not have upper limits on resources, so it does not support % rate limits for resources. ASA software also does not support limiting MAC addresses and IPSec tunnels.
URL-Server **url-server** *ifc name* **vendor websense host local_ip protocol tcp connections num_conns** **url-server /** *ifc name* **vendor websense host local_ip protocol udp context-name**	In FWSM release 4.0 in multiple context mode, this command can be sent to the websense server using the **context-name** keyword. Also, the **connections** keyword can be used to specify the number of simultaneous TCP connections without the **protocol** keyword.	ASA software does not support the **context-name** keyword. Also, it requires the **protocol** keyword, followed by TCP for configuring the number of simultaneous connections.