CHAPTER 5

cache through clear compression Commands

cache

To enter cache mode and set values for caching attributes, enter the **cache** command in webvpn mode. To remove all cache related commands from the configuration and reset them to default values, enter the **no** version of the command, also in webvpn mode.

cache

no cache

Defaults

Enabled with default settings for each cache attribute.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, with the result that many applications run much more efficiently.

Examples

The following example shows how to enter cache mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

cache-compressed

To cache compressed objects for WebVPN sessions, use the **cache-compressed** command in webvpn mode. To disallow caching of compressed content, enter the **no** version of the command.

cache-compressed enable

no cache-compressed

Syntax Description

enable	Enables caching of compressed content over WebVPN sessions.

Defaults

Caching of compressed content is enabled by default.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Cache mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Caching stores frequently reused objects in the system cache. When caching of compressed content is enabled, the security appliance stores compressed ojects. When you disable caching of compressed content, the security appliance stores objects prior to invoking the compression routine.

Examples

The following example shows how to disable caching of compressed content, and how to reenable it.

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# no cache-compressed
hostname(config-webvpn-cache)# cache-compressed enable
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.

Command	Description
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

cache-time

To specify in minutes how long to allow a CRL to remain in the cache before considering it stale, use the **cache-time** command in ca-crl configuration mode. To return to the default value, use the **no** form of this command.

cache-time *refresh-time*

no cache-time

Syntax Description

refresh-time	Specifies the number of minutes to allow a CRL to remain in the cache. The range is 1 - 1440 minutes. If the NextUpdate field is not present in the CRL, the CRL is not cached.

Defaults

The default setting is 60 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CRL configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and specifies a cache time refresh value of 10 minutes for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
enforcenextupdate	Specifies how to handle the NextUpdate CRL field in a certificate.

call-agent

To specify a group of call agents, use the **call-agent** command in MGCP map configuration mode, which is accessible by using the **mgcp-map** command. To remove the configuration, use the **no** form of this command.

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

Syntax Description

ip_address	The IP address of the gateway.
group_id	The ID of the call agent group, from 0 to 2147483647.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **call-agent** command to specify a group of call agents that can manage one or more gateways. The call agent group information is used to open connections for the call agents in the group (other than the one a gateway sends a command to) so that any of the call agents can send the response. Call agents with the same *group_id* belong to the same group. A call agent may belong to more than one group. The *group_id* option is a number from 0 to 4294967295. The *ip_address* option specifies the IP address of the call agent.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
```

```
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command. To disable packet capture capabilities, use the **no** form of this command (see the "Usage Guidelines" section for additional information about the **no** form of this command).

capture *capture_name* [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*] [**circular-buffer**]

capture *capture_name* **type asp-drop all** [*drop-code*] [**buffer** *buf_size*] [**circular-buffer**] [**packet-length** *bytes*]

capture *capture_name* **type isakmp** [**access-list** *access_list_name*] [**buffer** *buf_size*] [**circular-buffer**] [**interface** *interface_name*] [**packet-length** *bytes*]

capture *capture_name* **type raw-data** [**access-list** *access_list_name*] [**buffer** *buf_size*] [**circular-buffer**] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*]

capture *capture_name* **type webvpn user** *webvpn-user* [**url** *url*]

no capture *capture_name*

Syntax Description

access-list *access_list_name*	(Optional) Selects packets based on IP or higher fields for a specific access list identification.
all	Captures all the packets that the security appliance drops
buffer *buf_size*	(Optional) Defines the buffer size used to store the packet in bytes.
capture_name	Specifies the name of the packet capture.
circular-buffer	(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.
ethernet-type *type*	(Optional) Selects an Ethernet type to capture.
interface *interface_name*	(Optional) Specifies the interface on which to use packet capture, where *interface_name* is the name assigned to the interface by the **nameif** command. On ASA 5500 series adaptive security appliances, asa_dataplane is a valid value for *interface_name* and cofigures the security appliance to capture packets on the dataplane.
packet-length *bytes*	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
type asp-drop [*drop-code***]**	(Optional) Captures packets dropped for a reason. You can specify a particular reason by using the *drop-code* argument. Valid values for the *drop-code* argument are listed in the "Usage Guidelines" section, below.
type isakamp	(Optional) Captures encrypted and decrypted ISAKMP payloads.
type raw-data	(Optional) Captures inbound and outbound packets on one or more interfaces. This is the default.
type webvpn	(Optional) Captures WebVPN data for a specific WebVPN connection.
url *url*	(Optional) Specifies a URL for a WebVPN connection capture.
user *webvpn-user*	(Optional) Specifies a username for a WebVPN capture.

Defaults

The defaults are as follows:

- The capture type is raw data.
- The **buffer** *size* is 512 KB.
- All the Ethernet types are accepted.
- All the IP packets are matched.
- The **packet-length** is 1518 bytes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged mode	•	•	•	•	•

Command History

Release	Modification
6.2	Support for this command was introduced on the security appliance.
7.0	This commandwas modified to include several new keywords, most notably the **type asp-drop**, **type isakmp**, **type raw-data**, and **type webvpn** keywords.
7.1	This command was modified to include several new valid values for the *drop-code* argument.
7.2(4)	Added the **all** option to capture all packets that the security appliance drops.

Usage Guidelines

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. The security appliance can track packet information for traffic that passes through it, including management traffic and inspection engines. Packet information for all traffic that passes through the device can be captured.

To capture packets on the dataplane of an ASA 5500 series adaptive security appliance, you can use the **interface** keyword with asa_dataplane as the name of the interface.

With ISAKMP, the ISAKMP subsystem does not have access to the upper layer protocols. The capture is a pseudo capture, with the Physical, IP, and UDP layers combined together to satisfy a PCAP parser. The peer addresses are obtained from the SA exchange and are stored in the IP layer.

When selecting an Ethernet type to be included from capture, an exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner Ethernet type is used for matching. By default, all the Ethernet types are accepted.

Once the byte buffer is full, packet capture stops.

To enable packet capturing, attach the capture to an interface with the *interface* optional argument. Multiple **capture** command statements attach the capture to multiple interfaces.

If you copy the buffer contents to a TFTP server in ASCII format, you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and read it with TCPDUMP or Ethereal.

The **ethernet-type** and **access-list** optional keywords select the packets to store in the buffer. A packet must pass both the Ethernet and access list filters before the packet is stored in the capture buffer.

The **circular-buffer** keyword allows you to enable the capture buffer to overwrite itself, starting from the beginning, when the capture buffer is full.

Enter the **no capture** command with either the **access-list** or **interface** optional keyword unless you want to clear the capture itself. Entering **no capture** without optional keywords deletes the capture. If the **access-list** optional keyword is specified, the access list is removed from the capture and the capture is preserved. If the **interface** optional keyword is specified, the capture is detached from the specified interface and the capture is preserved.

Note The **capture** command is not saved to the configuration, and the **capture** command is not copied to the standby module during failover.

Use the **copy capture:** *capture_name* **tftp://server/***path* **[pcap]** command to copy capture information to a remote TFTP server.

Use the **https://***securityappliance-ip-address***/capture/***capture_name*[**/pcap**] command to see the packet capture information with a web browser.

If you specify the **pcap** optional keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)

When you enable WebVPN capture, the security appliance creates a pair of matching files: *capture name*_ORIGINAL.000 and *capture name*_MANGLED.000. For each subsequent capture, the security appliance generates additional matching pairs of files and increments the file extensions. *url* is the URL prefix to match for data capture. Use the URL http://*server*/*path* to capture HTTP traffic to the server. Use https://*server*/*path* to capture HTTPS traffic to the server.

Note Enabling WebVPN capture affects the performance of the security appliance. Be sure to disable the capture after you generate the capture files that you need for troubleshooting.

type asp-drop Drop Codes

The following table lists valid values for the optional *drop-code* argument that can follow the **type asp-drop** keyword.

Drop Code	Description
acl-drop	Flow is denied by access rule.
all	All packet drop reasons.
bad-crypto	Bad crypto return in packet.
bad-ipsec-natt	Bad IPSEC NATT packet.
bad-ipsec-prot	IPSEC not AH or ESP.
bad-ipsec-udp	Bad IPSEC UDP packet.
bad-tcp-cksum	Bad TCP checksum.
bad-tcp-flags	Bad TCP flags.
buffer	Configure size of capture buffer, default is 512 KB.
circular-buffer	Overwrite buffer from beginning when full, default is non-circular.

Drop Code	Description
conn-limit	Connection limit reached.
ctm-error	CTM returned error.
dns-guard-id-not-matched	DNS Guard id not matched.
dns-guard-out-of-app-id	DNS Guard out of app id.
dst-l2_lookup-fail	Dst MAC L2 Lookup Failed.
flow-expired	Expired flow.
fo-standby	Dropped by standby unit.
host-move-pkt	FP host move packet.
ifc-classify	Virtual firewall classification failed.
inspect-dns-id-not-matched	DNS Inspect id not matched.
inspect-dns-invalid-domain-label	DNS Inspect invalid domain label.
inspect-dns-invalid-pak	DNS Inspect invalid packet.
inspect-dns-out-of-app-id	DNS Inspect out of app id.
inspect-dns-pak-too-long	DNS Inspect packet too long.
inspect-icmp-error-different-embedded-conn	ICMP Error Inspect different embedded conn.
inspect-icmp-error-no-existing-conn	ICMP Error Inspect no existing conn.
inspect-icmp-out-of-app-id	ICMP Inspect out of app id.
inspect-icmp-seq-num-not-matched	ICMP Inspect seq num not matched.
inspect-icmpv6-error-invalid-pak	ICMPv6 Error Inspect invalid packet.
inspect-icmpv6-error-no-existing-conn	ICMPv6 Error Inspect no existing conn.
intercept-unexpected	Intercept unexpected packet.
interface-down	Interface is down.
invalid-app-length	Invalid app length.
invalid-encap	Invalid encapsulation.
invalid-ethertype	Invalid ethertype.
invalid-ip-addr	Invalid IP address.
invalid-ip-header	Invalid IP header.
invalid-ip-length	Invalid IP length.
invalid-ip-option	IP option configured drop.
invalid-tcp-hdr-length	Invalid tcp length.
invalid-tcp-pak	Invalid TCP packet.
invalid-udp-length	Invalid udp length.
ip-fragment	IP fragment (unsupported).
ips-fail-close	IPS card is down.
ips-request	IPS Module requested drop.
ipsec-clearpkt-notun	IPSEC Clear Pkt w/no tunnel.
ipsec-ipv6	IPSEC via IPV6.

Drop Code	Description
ipsec-need-sa	IPSEC SA Not negotiated yet.
ipsec-spoof	IPSEC Spoof detected.
ipsec-tun-down	IPSEC tunnel is down.
ipsecudp-keepalive	IPSEC/UDP keepalive message.
ipv6_fp-security-failed	IPv6 fastpath security checks failed.
ipv6_sp-security-failed	IPv6 slowpath security checks failed.
l2_acl	FP L2 rule drop.
l2_same-lan-port	L2 Src/Dst same LAN port.
large-buf-alloc-fail	FP fp large buffer alloc failed.
loopback-buffer-full	Loopback buffer full.
lu-invalid-pkt	Invalid LU packet.
mp-pf-queue-full	PF Module queue full.
mp-pf-unexpected	PF Module received unexpected data.
mp-svc-addr-renew-response	SVC Module received address renew response data frame.
mp-svc-bad-framing	SVC Module received badly framed data.
mp-svc-bad-length	SVC Module received bad data length.
mp-svc-compress-error	SVC Module compression error.
mp-svc-decompres-error	SVC Module decompression error.
mp-svc-delete-in-progress	SVC Module received data while connection was being deleted.
mp-svc-flow-control	SVC Module is in flow control.
mp-svc-no-channel	SVC Module does not have a channel for reinjection.
mp-svc-no-prepend	SVC Module does not have enough space to insert header.
mp-svc-no-session	SVC Module does not have a session.
mp-svc-unknown-type	SVC Module received unknown data frame.
mp-svc-unsupported-mac	SVC Module does not support 802.1Q.
natt-keepalive	NAT-T keepalive message.
no-adjacency	No valid adjacency.
no-mcast-entry	FP no mcast entry.
no-mcast-intrf	FP no mcast output intrf.
no-punt-cb	No registered punt cb.
no-route	No route to host.
non-ip-pkt-in-routed-mode	Non-IP packet received in routed mode.
np-socket-closed	Dropped pending packets in a closed socket.
np-sp-invalid-spi	Invalid SPI.

Drop Code	Description
packet-length	Configure maximum length to save from each packet, default is 68 bytes.
punt-rate-limit	Punt rate limit exceeded.
queue-removed	Queued packet dropped.
rate-exceeded	QoS rate exceeded.
rpf-violated	Reverse-path verify failed.
security-failed	Early security checks failed.
send-ctm-error	Send to CTM returned error.
sp-security-failed	Slowpath security checks failed.
ssm-app-fail	Service module is down.
ssm-app-request	Service module requested drop.
ssm-asdp-invalid	Invalid ASDP packet received from SSM card.
ssm-dpp-invalid	Invalid packet received from SSM card.
tcp-3whs-failed	TCP failed 3 way handshake.
tcp-ack-syn-diff	TCP ACK in SYNACK invalid.
tcp-acked	TCP DUP and has been ACKed.
tcp-bad-option-len	Bad option length in TCP.
tcp-bad-option-list	TCP option list invalid.
tcp-bad-sack-allow	Bad TCP SACK ALLOW option.
tcp-bad-winscale	Bad TCP window scale value.
tcp-buffer-full	TCP packet buffer full.
tcp-conn-limit	TCP Connection limit reached.
tcp-data-past-fin	TCP data send after FIN.
tcp-discarded-ooo	TCP packet out of order.
tcp-dual-open	TCP Dual open denied.
tcp-fo-drop	TCP replicated flow pak drop.
tcp-invalid-ack	TCP invalid ACK.
tcp-mss-exceeded	TCP MSS was too large.
tcp-mss-no-syn	TCP MSS option on non-SYN.
tcp-not-syn	First TCP packet not SYN.
tcp-paws-fail	TCP packet failed PAWS test.
tcp-reserved-set	TCP reserved flags set.
tcp-rst-syn-in-win	TCP RST/SYN in window.
tcp-rstfin-ooo	TCP RST/FIN out of order.
tcp-seq-past-win	TCP packet SEQ past window.
tcp-seq-syn-diff	TCP SEQ in SYN/SYNACK.
tcp-syn-data	TCP SYN with data.
tcp-syn-ooo	TCP SYN on established conn.

Drop Code	Description
tcp-synack-data	TCP SYNACK with data.
tcp-synack-ooo	TCP SYNACK on established conn.
tcp-tsopt-notallowed	TCP timestamp not allowed.
tcp-winscale-no-syn	TCP Window scale on non-SYN.
tcp_xmit_partial	TCP retransmission partial.
tcpnorm-rexmit-bad	TCP bad retransmission.
tcpnorm-win-variation	TCP unexpected window size variation.
tfw-no-mgmt-ip-config	No management IP address configured for TFW.
unable-to-add-flow	Flow hash full.
unable-to-create-flow	Out of flow cache memory.
unimplemented	Slow path unimplemented.
unsupport-ipv6-hdr	Unsupported IPV6.
unsupported-ip-version	Unsupported IP version.

Examples

To enable packet capture, enter the following:

```
hostname(config)# capture captest interface inside
hostname(config)# capture captest interface outside
```

On a web browser, the capture contents for a capture named “mycapture” can be viewed at the following location:

```
https://171.69.38.95/capture/mycapture/pcap
```

To download a libpcap file (used in web browsers such as Internet Explorer or Netscape Navigator) to a local machine, enter the following:

```
https://171.69.38.95/capture/http/pcap
```

This example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
hostname(config)# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname(config)# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname(config)# capture http access-list http packet-length 74 interface inside
```

This example shows how to capture ARP packets:

```
hostname(config)# capture arp ethernet-type arp interface outside
```

This example creates a WebVPN capture designated *hr*, which is configured to capture HTTP traffic for user2 visiting website wwwin.abcd.com/hr/people:

```
hostname# capture hr type webvpn user user2 url http://wwwin.abcd.com/hr/people
WebVPN capture started.
   capture name   hr
   user name      user2
   url            /http/0/wwwin.abcd.com/hr/people
hostname#
```

Related Commands

Command	Description
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.
show capture	Displays the capture configuration when no options are specified.

cd

To change the current working directory to the one specified, use the **cd** command in privileged EXEC mode.

cd [**flash:**] [*path*]

Syntax Description

flash:	Specifies the internal Flash memory, followed by a colon.
path	(Optional) The absolute path of the directory to change to.

Defaults

If you do not specify a directory, the directory is changed to the root directory.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows how to change to the “config” directory:

```
hostname# cd flash:/config/
```

Related Commands

Command	Description
pwd	Displays the current working directory.

certificate

To add the indicated certificate, use the **certificate** command in crypto ca certificate chain mode. When you use this command, the security appliance interprets the data included with it as the certificate in hexadecimal format. A **quit** string indicates the end of the certificate.

To delete the certificate, use the **no** form of the command.

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

certificate-serial-number	Specifies the serial number of the certificate in hexadecimal format ending with the word quit.
ca	Indicates that the certificate is a certificate authority (CA) issuing certificate.
ra-encrypt	Indicates that the certificate is a registration authority (RA) key encipherment certificate used in SCEP.
ra-general	Indicates that the certificate is a registration authority (RA) certificate used for digital signing and key encipherment in SCEP messaging.
ra-sign	Indicates that the certificate is an registration authority (RA) digital signature certificate used in SCEP messaging.

Defaults

This command has no default values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Certificate chain configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A certificate authority (CA) is an authority in a network that issues and manages security credentials and public key for message encryption. As part of a public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Examples

This example enters ca trustpoint mode for a trustpoint named central, then enters crypto ca certificate chain mode for central, and adds a CA certificate with a serial number 29573D5FF010FE25B45:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps
show running-config crypto map	Displays configuration for all crypto maps.
crypto ca certificate chain	Enters certificate crypto ca certificate chain mode.
crypto ca trustpoint	Enters ca trustpoint mode.

chain

To enable sending of a certificate chain, use the **chain** command in tunnel-group ipsec-attributes configuration mode. This action includes the root certificate and any subordinate CA certificates in the transmission. To return this command to the default, use the **no** form of this command.

chain

no chain

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all IPSec tunnel-group types.

Examples

The following example entered in tunnel-group-ipsec attributes configuration mode, enables sending a chain for an IPSec LAN-to-LAN tunnel group with the IP address of 209.165.200.225, which includes the root certificate and any subordinate CA certificates:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the current tunnel-group configuration.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

changeto

To change between security contexts and the system, use the **changeto** command in privileged EXEC mode.

changeto {**system** | **context** *name*}

Syntax Description

context *name*	Changes to the context with the specified name.
system	Changes to the system execution space.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you log into the system execution space or the admin context, you can change between contexts and perform configuration and monitoring tasks within each context. The "running" configuration that you edit in configuration mode, or that is used in the **copy** or **write** commands, depends on which execution space you are in. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context execution space, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) by entering the **show running-config** command. Only the current configuration appears.

Examples

The following example changes between contexts and the system in privileged EXEC mode:

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

The following example changes between the system and the admin context in interface configuration mode. When you change between execution spaces, and you are in a configuration submode, the mode changes to the global configuration mode in the new execution space.

```
hostname(config-if)# changeto context admin
hostname/admin(config)#
```

Related Commands

Command	Description
admin-context	Sets a context to be the admin context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

character-encoding

To specify the global character encoding in WebVPN portal pages, use the **character-encoding** command in webvpn configuration mode. The **no** form removes the value of the character-encoding attribute.

character-encoding *charset*

no character-encoding [*charset*]

Syntax Description

charset	String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850. The string is case-insensitive. The command interpreter converts upper-case to lower-case in the security appliance configuration.

Defaults

No default behavior or values. The encoding type set on the remote browser determines the character set for WebVPN portal pages when this attribute does not have a value.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Character encoding, also called “character coding” and “a character set,” is the pairing of raw data (such as 0’s and 1’s) and characters to represent the data. The language determines the character encoding method to use. Some languages use the same method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the user can change this. The browser can also detect the encoding specified on the page, and render the document accordingly. The character-encoding attribute lets you specify the value of the character-encoding method into the WebVPN portal page to ensure that the browser renders it properly, regardless of the region in which the user is using the browser, or any changes made to the browser.

The character-encoding attribute is a global setting that, by default, all WebVPN portal pages inherit. However, you can override the file-encoding attribute for Common Internet File System servers that use character encoding that differs from the value of the character-encoding attribute. You can use different file-encoding values for CIFS servers that require different character encodings.

The WebVPN portal pages downloaded from the CIFS server to the WebVPN user encode the value of the WebVPN file-encoding attribute identifying the server, or if one does not, they inherit the value of the character-encoding attribute. The remote user's browser maps this value to an entry in its character encoding set to determine the proper character set to use. The WebVPN portal pages do not specify a value if WebVPN configuration does not specify a file-encoding entry for the CIFS server and the character-encoding attribute is not set. The remote browser uses its own default encoding if the WebVPN portal page does not specify the character encoding or if it specifies a character encoding value that the browser does not support.

The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the proper rendering of file names or directory paths, as well as pages, are an issue.

Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

Examples

The following example sets the character-encoding attribute to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

Related Commands

Command	Description
file-encoding	Specifies CIFS servers and associated character encoding to override the value of this attribute.
show running-config [all] webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.
debug webvpn cifs	Displays debug messages about the CIFS.

checkheaps

To configure checkheaps verification intervals, use the **checkheaps** command in global configuration mode. To set the value to the default, use the **no** form of this command. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

Syntax Description

check-interval	Sets the buffer verification interval. The buffer verification process checks the sanity of the heap (allocated and freed memory buffers). During each invocation of the process, the security appliance checks the entire heap, validating each memory buffer. If there is a discrepancy, the security appliance issues either an "allocated buffer error" or a "free buffer error." If there is an error, the security appliance dumps traceback information when possible and reloads.
validate-checksum	Sets the code space checksum validation interval. When the security appliance first boots up, the security appliance calculates a hash of the entire code. Later, during the periodic check, the security appliance generates a new hash and compares it to the original. If there is a mismatch, the security appliance issues a "text checksum checkheaps error." If there is an error, the security appliance dumps traceback information when possible and reloads.
seconds	Sets the interval in seconds between 1 and 2147483.

Defaults

The default intervals are 60 seconds each.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the buffer allocation interval to 200 seconds and the code space checksum interval to 500 seconds:

```
hostname(config)# checkheaps check-interval 200
hostname(config)# checkheaps validate-checksum 500
```

Related Commands

Command	Description
show checkheaps	Shows checkheaps statistics.

check-retransmission

To prevent against TCP retransmission style attacks, use the **check-retransmission** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

check-retransmission

no check-retransmission

Syntax Description

This command has no arguments or keywords.

Defaults

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. To prevent against TCP retransmission style attacks that arise from end-system interpretation of inconsistent retransmissions, use the **check-retransmission** command in tcp-map configuration mode.

The security appliance will make efforts to verify if the data in retransmits are the same as the original. If the data doesn't match, then the connection is dropped by the security appliance. When this feature is enabled, packets on the TCP connection are only allowed in order. For more details, see the **queue-limit** command.

Examples

The following example enables the TCP check-retransmission feature on all TCP flows:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
```

```
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

checksum-verification

To enable or disable TCP checksum verification, use the **checksum-verification** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

checksum-verification

no checksum-verification

Syntax Description

This command has no arguments or keywords.

Defaults

Checksum verification is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **checksum-verification** command in tcp-map configuration mode to enable TCP checksum verification. If the check fails, the packet is dropped.

Examples

The following example enables TCP checksum verification on TCP connections from 10.0.0.0 to 20.0.0.0:

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap

hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

class (policy-map)

To assign a class-map to a policy for traffic classification, use the **class** command in policy-map mode. To remove a class-map specification for a policy map, use the **no** form of this command.

class *classmap-name*

no class *classmap-name*

Syntax Description

classmap-name	The name for the class-map. The name can be up to 40 characters long.

Defaults

By default, "class class-default" always exists at the end of a policy map.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy-map	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Including the class-default, up to 63 class commands can be configured in a policy map.

The name "class-default" is a reserved name for default class, and it always exists; that is, you can include it in your configuration, but you cannot reconfigure or remove it using CLI. See the description of the **class-map** command for more information.

Use the **class** command to enter class mode, in which you can enter the following commands:

set connection

inspect

ips

priority

police

See the individual command descriptions for detailed information.

Examples

The following is an example of the class command in policy-map mode; note the change in the prompt:

```
hostname(config)# class-map localclass1
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map localpolicy1
```

```
hostname(config-pmap)# class localclass1
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# exit
```

The following is an example of a **policy-map** command, with its **class** commands, for a connection policy that limits connections to an HTTP server to a maximum of 256:

```
hostname(config)# access-list myhttp permit tcp any host 10.1.1.1
hostname(config)# class-map myhttp

hostname(config-cmap)# match access-list myhttp
hostname(config-cmap)# exit

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class myhttp
hostname(config-pmap-c)# set connection conn-max 256
```

The following is an example of a **policy-map** command, with its **class** commands, for the outside interface (defined in the **service-policy** command). The **class-map** command specifies a class of traffic that has a destination IP address of 192.168.10.10:

```
hostname(config)# class-map outside-voip
hostname(config-cmap)# match dscp af11
hostname(config-cmap)# exit

hostname(config)# policy-map outside-policy
hostname(config-pmap)# description This policy map defines policies for the outside
interface.
hostname(config-pmap)# class outside-voip
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy outside-policy interface outside
```

Related Commands

Command	Description
clear configure policy-map	Removes all policy-map configuration, except for any policy-map that is in use in a service-policy command.
policy-map	Configures a policy; that is, an association of one or more traffic classes, each with one or more actions.
show running-config policy-map	Displays all current policy-map configurations.

class-map

To classify traffic for an interface when using Modular Policy Framework to configure a security feature, use the **class-map** command in global configuration mode. To delete a class map, use the **no** form of this command.

class-map *class_map_name*

no class-map *class_map_name*

Syntax Description

class_map_name	Text for the class map name; the text can be up to 40 characters in length. The name space for class-map is local to a security context. Therefore, the same name may be used in multiple security contexts. The maximum number of class-maps per security context is 255.

Defaults

The default class, class-default, always exists and cannot be configured or removed using the CLI. A default class, when used in a policy map, means "all other traffic.". The definition of class-default is:

```
class-map class-default
    match any
```

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **class-map** command allows you to define a traffic class when using Modular Policy Framework to configure a security feature. Modular Policy Framework provides a consistent and flexible way to configure security appliance features in a manner similar to Cisco IOS software QoS CLI. Use the **class-map**, **policy-map**, and **service-policy** global configuration commands to configure a security feature using Modular Policy Framework.

Define a traffic class using the **class-map** global configuration command. Then create a policy map by associating the traffic class with one or more actions using the **policy-map** global configuration command. Finally, create a security policy by associating the policy map with one or more interfaces using the **service-policy** command.

A traffic class map contains, at most, one **match** command (with the exception of the **match tunnel-group** and **match default-inspection-traffic** commands). The **match** command identifies the traffic included in the traffic class. When a packet is matched against a class-map, the match result is either a match or a no match.

Use the **class-map** command to enter class-map configuration mode. From class-map configuration mode, you can define the traffic to include in the class using the **match** command. The following commands are available in class-map configuration mode:

description	Specifies a description for the class-map.
match access-list	Specifies the name of an access-list to be used as match criteria. When a packet does not match an entry in the access-list, the match result is a no-match. When a packet matches an entry in an access-list, and if it is a permit entry, the match result is a match. Otherwise, if it matches a deny access-list entry, the match result is no-match.
match port	Specifies to match traffic using a TCP/UDP destination port.
match precedence	Specifies to match the precedence value represented by the TOS byte in the IP header.
match dscp	Specifies to match the IETF-defined DSCP value in the IP header.
match rtp	Specifies to match an RTP port.
match tunnel-group	Specifies to match security related tunnel groups.
match flow ip destination-address	Specifies to match the IP destination address.
match default-inspection-traffic	Specifies to match default traffic for the **inspect** commands.

Examples

The following example shows how to define a traffic class of all TCP traffic to port 21 using a class map:

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
```

Related Commands

Command	Description
clear configure class-map	Removes all of the traffic map definitions.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

clear aaa local user fail-attempts

To reset the number of failed user authentication attempts to zero without modifying the user's locked-out status, use the **clear aaa local user fail-attempts** command in privileged EXEC mode.

clear aaa local user authentication fail-attempts {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
name	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use this command when a user fails authentication a few times, but you want to reset to counter to zero, for example, when the configuration has recently been modified.

After the configured number of failed authentication attempts, the user is locked out of the system and cannot successfully log in until either a system administrator unlocks the username or the system reboots.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the security appliance reboots.

Locking or unlocking a username results in a syslog message.

A system administrator with a privilege level of 15 cannot be locked out.

Examples

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for all users:

```
hostname(config)# clear aaa local user authentication fail-attempts all
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
clear aaa local user lockout	Resets the number of failed user authentication attempts to zero without modifying the user's locked-out status.
show aaa local user [locked]	Shows the list of usernames that are currently locked.

clear aaa local user lockout

To clear the lockout status of the specified users and set their failed-attempts counter to 0, use the **clear aaa local user lockout** command in privileged EXEC mode.

clear aaa local user lockout {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
name	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can specify a single user by using the **username** option or all users with the **all** option.

This command affects only the status of users that are locked out.

The administrator cannot be locked out of the device.

Locking or unlocking a username results in a syslog message.

Examples

The following example shows use of the **clear aaa local user lockout** command to clear the lockout condition and reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user lockout username anyuser
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the user's locked-out status.
show aaa local user [locked]	Shows the list of usernames that are currently locked.

clear aaa-server statistics

To reset the statistics for AAA servers, use the **clear aaa-server statistics** command in privilged EXEC mode.

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

LOCAL	(Optional) Clears statistics for the LOCAL user database.
groupname	(Optional) Clears statistics for servers in a group.
host *hostname*	(Optional) Clears statistics for a particular server in the group.
protocol *protocol*	(Optional) Clears statistics for servers of the specificed protocol: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Defaults

Remove all AAA-server statistics across all groups.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines. In the protocol values, **nt** replaces the older **nt-domain**, and **sdi** replaces the older **rsa-ace**.

Examples

The following command shows how to reset the AAA statistics for a specific server in a group:

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

The following command shows how to reset the AAA statistics for an entire server group:

```
hostname(config)# clear aaa-server statistics svrgrp1
```

The following command shows how to reset the AAA statistics for all server groups:

```
hostname(config)# clear aaa-server statistics
```

The following command shows how to reset the AAA statistics for a particular protocol (in this case, TACACS+):

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

Related Commands

Command	Description
aaa-server protocol	Specifies and manages the grouping of AAA server connection data.
clear configure aaa-server	Removes all non-default aaa server groups or clear the specified group
show aaa-server	Displays AAA server statistics.
show running-config aaa-server	Displays the current AAA server configuration values.

clear access-group

To remove access groups from all the interfaces, use the **clear access-group** command.

clear access-group

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Prexisting	This command was preexisting.

Examples

The following example shows how to remove all access groups:

```
hostname(config)# clear access-group
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
show running-config access-group	Displays the current access group configuration.

clear access-list

To clear an access-list counter, use the **clear access-list** command in global configuration mode.

clear access-list [*id*] **counters**

Syntax Description

counters	Clears access list counters.
id	(Optional) Name or number of an access list.

Defaults

All the access list counters are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When you enter the **clear access-list** command, all the access list counters are cleared if you do not specify an *id*.

Examples

The following example shows how to clear a specific access list counter:

```
hostname# clear access-list inbound counters
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the access list configuration that is running on the security appliance.

clear arp

To clear dynamic ARP entries or ARP statistics, use the **clear arp** command in privileged EXEC mode.

clear arp [**statistics**]

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears all ARP statistics:

```
hostname# clear arp statistics
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear asp drop

To clear accelerated security path drop statistics, use the **clear asp drop** command in privileged EXEC mode.

clear asp drop [**flow** *type* | **frame** *type*]

Syntax Description

flow	(Optional) Clears the dropped flow statistics.
frame	(Optional) Clears the dropped packet statistics.
type	(Optional) Clears the dropped flow or packets statistics for a particular process. See "Usage Guidelines" for a list of types.

Defaults

By default, this command clears all drop statistics.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Process types include the following:

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
```

```
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

Examples

The following example clears all drop statistics:

```
hostname# clear asp drop
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

clear asp table

To clear the hit counters either in asp arp or classify tables, or both, use the **clear asp table** command in privileged EXEC mode.

clear asp table [**arp** | **classify**]

Syntax Description

arp	clears the hits counters in asp arp table only.
classify	clears the hits counters in asp classify tables only

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(4)	This command was introduced.

Usage Guidelines

There are only two options arp and classify having hits in the **clear asp table** command

Examples

The following example clears all drop statistics:

```
hostname# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! hostname#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands! hostname#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! hostname(config)# clear
asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! hostname# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

Related Commands

Command	Description
show asp table arp	Shows the contents of the accelerated security path, which might help you troubleshoot a problem.

clear blocks

To reset the packet buffer counters such as the low watermark and history information, use the **clear blocks** command in privileged EXEC mode.

clear blocks

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Resets the low watermark counters to the current available blocks in each pool. Also clears the history information stored during the last buffer allocation failure.

Examples

The following example clears the blocks:

```
hostname# clear blocks
```

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics
show blocks	Shows the system buffer utilization.

clear-button

To customize the Clear button of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **clear-button** command from webvpn customization mode:

clear-button {**text** | **style**} *value*

[**no**] **clear-button** {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default text is “Clear”.

The default style is border:1px solid black;background-color:white;font-weight:bold;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the default background color of the Clear button from black to blue:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# clear-button style background-color:blue
```

Related Commands

Command	Description
login-button	Customizes the login button of the WebVPN page Login box.
login-title	Customizes the title of the WebVPN page Login box.
group-prompt	Customizes the group prompt of the WebVPN page Login box.
password-prompt	Customizes the password prompt of the WebVPN page Login box.
username-prompt	Customizes the username prompt of the WebVPN page Login box.

clear capture

To clear the capture buffer, use the **clear capture** *capture_name* command.

clear capture *capture_name*

Syntax Description

capture_name	Name of the packet capture.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Priveleged Mode	•	•	•	•	•

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the security appliance.

Usage Guidelines

The shortened form of the **clear capture** (for example, **cl cap** or **clear cap**) is not supported to prevent accidental destruction of all the packet captures.

Examples

This example shows how to clear the capture buffer for the capture buffer “trudy”:

```
hostname(config)# clear capture trudy
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
show capture	Displays the capture configuration when no options are specified.

clear compression

To clear compression statistics for all SVC and WebVPN connections, use the **clear compression** command from privileged EXEC mode:

clear compression {**all** | **svc** | **http-comp**}

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

In the following example, the user clears the compression configuration:

```
hostname#(config) clear configure compression
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of data over an SVC connection for a specific group or user.