



show running-config same-security-traffic through show running-config xlate Commands

show running-config same-security-traffic

To display the same-security interface communication, use the **show running-config same-security-traffic** command in privileged EXEC mode.

show running-config same-security-traffic

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:

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

Release	Modification
7.0(1)	This command was introduced.

Examples The following is sample output from the **show running-config same-security-traffic** command:

```
hostname# show running-config same-security-traffic
```

Command	Description
same-security-traffic	Permits communication between interfaces with equal security levels.

show running-config service

To display the system services, use the **show running-config service** command in privileged EXEC mode.

show running-config service

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:

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

Command History	Release	Modification
	7.0(1)	The keyword running-config was added.

Examples This command shows how to display the system services:

```
hostname# show running-config service
service resetoutside
```

Related Commands	Command	Description
	service	Enables system services.

show running-config service-policy

To display all currently running service policy configurations, use the **show running-config service-policy** command in privileged EXEC mode.

show running-config [all] service-policy

Syntax Description

all (Optional) Shows all service policy commands, including the commands you have not changed from the default.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output of the **show running-config service-policy** command:

```
hostname# show running-config service-policy
```

Related Commands

Command	Description
show service-policy	Displays the service policy.
service-policy	Configures service policies.
clear service-policy	Clears service policy configurations.
clear configure service-policy	Clears service policy configurations.

show running-config sla monitor

To display the SLA operation commands in the running configuration, use the **show running-config sla monitor** command in privileged EXEC mode.

show running-config sla monitor [*sla-id*]

Syntax Description

sla_id Specifies the SLA ID for the **sla monitor** commands being displayed. Valid values are from 1 to 2147483647.

Defaults

If the *sla-id* is not specified, the **sla monitor** commands for all SLA operations are displayed.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines


This command displays the **sla monitor** commands, associated SLA monitor configuration mode commands, and the associated **sla monitor** schedule command, if present. It does not display the **track rtr** commands in the configuration.

Examples

The following is sample output from the **show running-config sla monitor 5** command. It displays the SLA monitor configuration for the SLA operation with the SLA ID of 5:

```
hostname# show running-config sla monitor 5

sla monitor 124
  type echo protocol ipIcmpEcho 10.1.1.1 interface outside
  timeout 1000
  frequency 3
sla monitor schedule 124 life forever start-time now
```

 show running-config sla monitor

Related Commands	Command	Description
	clear configure sla monitor	Removes the sla monitor , and associated commands, from the running configuration.
	show sla monitor configuration	Displays configuration values for the specified SLA operation.

show running-config smtps

To display the running configuration for SMTPS, use the **show running-config smtps** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-config [all] smtps

Syntax Description	all	Displays the running configuration including default values.
---------------------------	------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

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

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

Command History	Release	Modification
	7.0(1)	This command was introduced.

Examples	The following is sample output from the show running-config smtps command:
-----------------	---

```
hostname# show running-config smtps

smtps
server 10.1.1.21
authentication-server-group KerbSvr
authentication aaa

hostname# show running-config all smtps

smtps
port 995
server 10.1.1.21
outstanding 20
name-separator :
server-separator @
authentication-server-group KerbSvr
no authorization-server-group
no accounting-server-group
no default-group-policy
authentication aaa
hostname#
```

show running-config snmp-map

To show the SNMP maps that have been configured, use the **show running-config snmp-map** command in privileged EXEC mode.

show running-config snmp-map *map_name*

Syntax Description.

map_name Displays the configuration for the specified SNMP map.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config snmp-map** command displays the SNMP maps that have been configured.

Examples

The following is sample output from the **show running-config snmp-map** command:

```
hostname# show running-config snmp-map snmp-policy
!
snmp-map snmp-policy
deny version 1
!
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enables SNMP application inspection.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.

show running-config snmp-server

To display all currently running SNMP server configurations, use the **show running-config snmp-server** command in global configuration mode.

show running-config snmp-server [default] [group | host | user]

Syntax Description

default	Displays the default SNMP server configuration.
group	Displays the SNMP group configurations.
host	Displays the SNMP host configurations.
user	Displays the SNMP user configurations.

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
7.0(1)	This command was introduced.

Usage Guidelines

This command does not display output for the **snmp-server trap** commands for the default traps; output is displayed only for the enabled, non-default traps. The **no snmp-server trap** command is also displayed for the disabled default traps.

The following is sample output from the **show running-config snmp-server** command:

```
hostname# show running-config snmp-server
snmp-server host inside 10.21.104.209 community asa1
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

Related Commands

Command	Description
snmp-server	Configures the SNMP server.
clear configure snmp-server	Clears the SNMP server configuration.
show snmp-server statistics	Displays the SNMP server configuration.

show running-config ssh

To show the SSH commands in the current configuration, use the **show running-config ssh** command in privileged EXEC mode.

show running-config [**default**] **ssh** [**timeout** | **version**]

show run [**default**] **ssh** [**timeout**]

Syntax Description

default	(Optional) Displays the default SSH configuration values along with the configured values.
timeout	(Optional) Displays the current SSH session timeout value.
version	(Optional) Displays the version of SSH currently being supported.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The command was changed from the show ssh command to the show running-config ssh command.

Usage Guidelines

This command shows the current ssh configuration. To display only the SSH session timeout value, use the **timeout** option. To see a list of active SSH sessions, use the **show ssh sessions** command.

Examples

The following example displays the SSH session timeout:

```
hostname# show running-config timeout
ssh timeout 5 minutes
hostname#
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
ssh	Allows SSH connectivity to the ASA from the specified client or network.

Command	Description
ssh scopy enable	Enables a secure copy server on the ASA.
ssh timeout	Sets the timeout value for idle SSH sessions.
ssh version	Restricts the ASA to using either SSH Version 1 or SSH Version 2.

show running-config ssh key-exchange

To show which (Diffie-Hellman) key-exchange method can be used for SSH sessions, use the **show running-config ssh key-exchange** command in privileged EXEC mode.

show running-config ssh key-exchange

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:

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

Command History

Release	Modification
8.4(5)	This command was introduced.

Usage Guidelines

This command shows the current SSH key exchange configuration.

Examples

The following example displays the SSH key exchange configuration:

```
hostname# show running-config ssh key-exchange
ssh key-exchange group dh-group14-sha1
hostname#
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
ssh	Allows SSH connectivity to the ASA from the specified client or network.
ssh scopy enable	Enables a secure copy server on the ASA.
ssh timeout	Sets the timeout value for idle SSH sessions.
ssh version	Restricts the ASA to using either SSH Version 1 or SSH Version 2.

show running-config ssl

To display the current set of configured ssl commands, use the **show running-config ssl** command in privileged EXEC mode.

show running-config ssl

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config ssl** command:

```
hostname# show running-config ssl
ssl server-version tlsrv1
ssl client-version tlsrv1-only
ssl encryption 3des-sha1
ssl trust-point Firstcert
```

Related Commands

Command	Description
clear config ssl	Removes all ssl commands from the configuration, reverting to the default values.
ssl client-version	Specifies the SSL/TLS protocol version the ASA uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the ASA uses when acting as a server
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

show running-config static

To display all **static** commands in the configuration, use the **show running-config static** command in privileged EXEC mode.

show running-config static

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:

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

Command History

Release	Modification
7.0(1)	The keyword running-config was added.

Usage Guidelines

This command displays the maximum connections value for the UDP protocol. If the UDP maximum connections value is “0” or not set, the limit enforcement is disabled.

Examples

This example shows how to display all static commands in the configuration:

```
hostname# show running-config static
static (inside,outside) 192.150.49.91 10.1.1.91 netmask 255.255.255.255
static (inside,outside) 192.150.49.200 10.1.1.200 netmask 255.255.255.255 tcp 255 0
```



Note

No UDP value connection limit is shown.

Related Commands

Command	Description
clear configure static	Removes all the static commands from the configuration.
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

show running-config sunrpc-server

To display the information about the SunRPC configuration, use the **show running-config sunrpc-server** command in privileged EXEC mode.

show running-config sunrpc-server *interface_name* *ip_addr* *mask* **service** *service_type* **protocol** [TCP | UDP] **port** *port* [- *port*] **timeout** *hh:mm:ss*

Syntax Description	
<i>interface_name</i>	Server interface.
<i>ip_addr</i>	Server IP address.
<i>mask</i>	Network mask.
port <i>port</i> - <i>port</i>	SunRPC protocol port range and optionally, a second port.
protocol	SunRPC transport protocol.
service	Specifies a service.
<i>service_type</i>	Sets the SunRPC service program type.
timeout <i>hh:mm:ss</i>	Specifies the timeout idle time after which the access for the SunRPC service traffic is closed.
TCP	(Optional) Specifies TCP.
UDP	(Optional) Specifies UDP.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0(1)	This command was introduced.

Usage Guidelines The *service_type* is specified in the **sunrpcinfo** command.

Examples The following is sample output from the **show running-config sunrpc-server** command:

```
hostname# show running-config sunrpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout 0:03:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the SunRPC services from the ASA.
debug sunrpc	Enables debug information for SunRPC.
show conn	Displays the connection state for different connection types, including SunRPC.
sunrpc-server	Creates the SunRPC services table.
timeout	Sets the maximum idle time duration for different protocols and session types, including SunRPC.

show running-config sysopt

To show the **sysopt** command configuration in the running configuration, use the **show running-config sysopt** command in privileged EXEC mode.

show running-config sysopt

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:

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

Command History

Release	Modification
7.0(1)	This command was changed from the show sysopt command.

Examples

The following is sample output from the **show running-config sysopt** command:

```
hostname# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1200
sysopt connection tcpmss minimum 400
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-ipsec
```

Related Commands

Command	Description
clear configure sysopt	Clears the sysopt command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the alias command.

show running-config tcp-map

To display the information about the TCP map configuration, use the **show running-config tcp-map** command in privileged EXEC mode.

show running-config tcp-map [*tcp_map_name*]

Syntax Description

tcp_map_name (Optional) Text for the TCP map name; the text can be up to 58 characters in length.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config tcp-map** command:

```
hostname# show running-config tcp-map
tcp-map localmap
```

Related Commands

Command	Description
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.
clear configure tcp-map	Clears the TCP map configuration.

show running-config telnet

To display the current list of IP addresses that are authorized to use Telnet connections to the ASA, use the **show running-config telnet** command in privileged EXEC mode. You can also use this command to display the number of minutes that a Telnet session can remain idle before being closed by the ASA.

show running-config telnet [timeout]

Syntax Description	timeout	(Optional) Displays the number of minutes that a Telnet session can be idle before being closed by the ASA.
--------------------	---------	---

Defaults	No default behavior or values.
----------	--------------------------------

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

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

Command History	Release	Modification
	7.0(1)	The keyword running-config was added.

Examples	This example shows how to display the current list of IP addresses that are authorized for use by Telnet connections to the ASA:
----------	--

```
hostname# show running-config telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User  failed to
log in from 128.107.183.22 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User  failed to log in from 128.107.183.
22 through Telnet
```

Related Commands	Command	Description
	clear configure telnet	Removes the Telnet connection from the configuration.
	telnet	Adds Telnet access to the console and sets the idle timeout.

show running-config terminal

To display the current terminal settings, use the **show running-config terminal** command in privileged EXEC mode.

show running-config terminal

Syntax Description This command has no arguments or keywords.

Defaults The default display width is 80 columns.

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

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

Release	Modification
7.0(1)	This command was introduced.

Command History

Examples The following example clears the page length setting:

```
hostname# show running-config terminal
```

```
Width = 80, no monitor
```

Command	Description
clear configure terminal	Clears the terminal display width setting.
terminal	Sets the terminal line parameters.
terminal width	Sets the terminal display width.

Related Commands

show running-config tftp-server

To display the default TFTP server address and directory, use the **show running-config tftp-server** command in global configuration mode.

show running-config tftp-server

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
	7.0(1)	The running-config keyword was added.

Examples This example shows how to display the IP/IPv6 address of the default TFTP server and the directory of the configuration file:

```
hostname(config)# show running-config tftp-server
tftp-server inside 10.1.1.42 /temp/config/test_config
```

Related Commands	Command	Description
	configure net	Loads the configuration from the TFTP server and path you specify.
	tftp-server	Configures the default TFTP server address and the directory of the configuration file.

show running-config threat-detection

To view the threat detection configuration, use the **show running-config threat-detection** command in privileged EXEC mode.

show running-config [**all**] **threat-detection** [**basic-threat** | **rate** | **scanning-threat** | **statistics** | **tcp-intercept**]

Syntax Description

all	(Optional) Shows all threat detection commands, including the commands you have not changed from the default. For example, you can view the default rate limits for the threat-detection basic-threat command.
basic-threat	(Optional) Shows the basic threat configuration.
rate	(Optional) Shows the rate configuration.
scanning-threat	(Optional) Shows the scanning threat configuration.
statistics	(Optional) Shows the statistics configuration.
tcp-intercept	(Optional) Shows the statistics configuration for TCP Intercept.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	The tcp-intercept keyword was added.

Examples

The following is sample output from the **show running-config all threat-detection** command, which shows the default rate limits for the **threat-detection basic-threat** command:

```
hostname# show running-config all threat-detection
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 400 burst-rate 800
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
```

```

threat-detection rate icmp-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate scanning-drop rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-drop rate-interval 3600 average-rate 5 burst-rate 10
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 100 burst-rate 200
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 400 burst-rate 1600
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 2000 burst-rate 8000
threat-detection scanning-threat shun duration 3600
threat-detection statistics
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200

```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

show running-config timeout

To display the timeout value of all protocols, or just a specific one, use the **show running-config timeout** command in privileged EXEC mode.

show running-config timeout *protocol*

Syntax Description

protocol (Optional) Displays the timeout value of the specified protocol. Supported protocols are: **xlate**, **conn**, **udp**, **icmp**, **rpc**, **h323**, **h225**, **mgcp**, **mgcp-pat**, **sip**, **sip_media**, and **uauth**.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The running-config and mgcp-pat keywords were added.

Examples

This example shows how to display the timeout values for the system:

```
hostname(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
```

Related Commands

Command	Description
clear configure timeout	Restores the default idle time durations.
timeout	Sets the maximum idle time duration.

show running-config tls-proxy

To display all currently running TLS proxy configurations, use the **show running-config tls-proxy** command in privileged EXEC mode.

show running-config [**all**] **tls-proxy** [*proxy_name*]

Syntax Description

all	Shows all TLS proxy commands, including the commands you have not changed from the default.
<i>proxy_name</i>	Specifies the name of the TLS proxy to show.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following is sample output of the **show running-config all tls-proxy** command:

```
hostname# show running-config tls-proxy
tls-proxy proxy
  server trust-point local_ccm
  client ldc issuer ldc_signer
  client ldc key-pair phone_common
  no client cipher-suite
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show tls-proxy	Shows all TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

show running-config track

To display **track rtr** commands in the running configuration, use the **show running-config track** command in privileged EXEC mode.

show running-config track [*track-id*]

Syntax	Description
<i>track-id</i>	(Optional) Limits the display to the track rtr command with the specified tracking object ID.

Defaults If the *track-id* is not specified, all **track rtr** commands in the running configuration are shown.

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

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

Command History	Release	Modification
	7.2(1)	This command was introduced.

Examples The following is sample output from the **show running-config track** command:

```
hostname# show running-config track 5
track 5 rtr 124 reachability
```

Related Commands	Command	Description
	clear configure track	Removes the track rtr commands from the running configuration.
	show track	Displays information about the objects being tracked.
	track rtr	Creates a tracking entry to poll the SLA.

show running-config tunnel-group

To display tunnel group information about all or a specified tunnel group and tunnel-group attributes, use the **show running-config tunnel-group** command in global configuration or privileged EXEC mode.

show running-config [**all**] **tunnel-group** [*name* [**general-attributes** | **ipsec-attributes** | **ppp-attributes**]]

Syntax Description

all	[Optional] Displays all tunnel-group commands, including the commands you have not changed from the default.
general-attributes	Displays configuration information for general attributes.
ipsec-attributes	Displays configuration information for IPSec attributes.
<i>name</i>	Specifies the name of the tunnel group.
ppp-attributes	Displays configuration information for PPP attributes.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays the current configuration for all tunnel groups:

```
hostname(config)# show running-config tunnel-group
tunnel-group 209.165.200.225 type IPSec_L2L
tunnel-group 209.165.200.225 ipsec-attributes
    pre-shared-key xyzx
hostname(config)#
```

Related Commands	Command	Description
	clear configure tunnel-group	Removes tunnel-group configuration
	tunnel-group general-attributes	Enters subconfiguration mode for specifying general attributes for specified tunnel group.
	tunnel-group ipsec-attributes	Enters subconfiguration mode for specifying IPSec attributes for specified tunnel group.
	tunnel-group	Enters tunnel-group subconfiguration mode for the specified type.

show running-config url-block

To show the configuration for buffers and memory allocation used by URL filtering, use the **show running-config url-block** command in privileged EXEC mode.

show running-config url-block [block | url-mempool | url-size]

Syntax Description

block	Displays the configuration for the maximum number of blocks that will be buffered.
url-mempool	Displays the configuration for the maximum allow URL size (in KB).
url-size	Displays the configuration for the memory resource (in KB) allocated for the long URL buffer.

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

The **show running-config url-block** command displays the configuration for buffers and memory allocation used by URL filtering.

Examples

The following is sample output from the **show running-config url-block** command:

```
hostname# show running-config url-block
!
url-block block 56
!
```

Related Commands	Commands	Description
	clear url-block block statistics	Clears the block buffer usage counters.
	show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
	url-block	Manage the URL buffers used for web server responses.
	url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
	url-server	Identifies an N2H2 or Websense server for use with the filter command.

show running-config url-cache

To show the cache configuration used by URL filtering, use the **show running-config url-cache** command in privileged EXEC mode.

show running-config url-cache

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config url-cache** command displays the cache configuration used by URL filtering.

Examples

The following is sample output from the **show running-config url-cache** command:

```
hostname# show running-config url-cache
!
url-cache src_dst 128
!
```

Related Commands

Commands	Description
clear url-cache statistics	Removes url-cache command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show running-config url-server

To show the URL filtering server configuration, use the **show running-config url-server** command in privileged EXEC mode.

show running-config url-server

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config url-server** command displays the URL filtering server configuration.

Examples

The following is sample output from the **show running-config url-server** command:

```
hostname# show running-config url-server
!
url-server (perimeter) vendor websense host 10.0.1.1
!
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show running-config user-identity

To display the configuration for the Identity Firewall, use the **user-identity poll-import-user-group-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

show running-config user-identity [**ad-agent** | **logout-probe** | **action** | **default-domain** | **domain** *domain_nickname*]

Syntax Description		
action		Displays the configuration for the following Identity Firewall actions configured by the following commands: <ul style="list-style-type: none"> user-identity action ad-agent-down user-identity action domain-controller-down user-identity action mac-address-mismatch user-identity action netbios-response-fail
ad-agent		Displays all configuration for the Active Directory Agent configured for the Identity Firewall.
<i>domain_nickname</i>		Displays the configuration for the domain specified by the <i>domain_nickname</i> argument.
default-domain		Specifies the configuration for the Identity Firewall default domain. You configure the default domain by entering the user-identity default-domain command.
domain		Displays all domains configured for the Identity Firewall.
logout-probe		Displays all configuration for the logout probe configured for the Identity Firewall. <p>When NetBIOS probing is enabled for the Identity Firewall, the ASA probes the user client IP address to determine whether the client is still active. By default, NetBIOS probing is disabled.</p>

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	8.4(2)	The command was introduced.

Examples

The following example displays the configuration for the Active Directory Agent configured for the Identity Firewall:

```
hostname(config)# show running-config user-identity ad-agent
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

show running-config username

To display the running configuration for a particular user, use the **show running-config username** command in privileged EXEC mode with the username appended. To display the running configuration for all users, use this command without a username.

show running-config [**all**] **username** [*name*] [**attributes**]

Syntax Description

attributes	Displays the specific AVPs for the user(s)
all	(Optional) Displays all username commands, including the commands that you have not changed from the default settings.
<i>name</i>	Provides the name of the user.

Defaults

No default behavior or values.

Command Modes

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

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


Command History

Release	Modification
7.0(1)	This command was introduced.
8.4.4(1)	The output for the show running-config all username command was updated to add password date information.

Examples

The following is sample output from the **show the running-config username** command for a user named anyuser:

```
hostname# show running-config username anyuser
username anyuser password .8T1d6ik58/lzXS5 encrypted privilege 3
username anyuser attributes
vpn-group-policy DefaultGroupPolicy
vpn-idle-timeout 10
vpn-session-timeout 120
vpn-tunnel-protocol IPSec
```

 show running-config username**Related Commands**

Command	Description
clear config username	Clears the username database.
username	Adds a user to the ASA database.
username attributes	Lets you configure attributes for specific users.

show running-config virtual

To display the IP address of the ASA virtual server, use the **show running-config virtual** command in privileged EXEC mode.

show running-config [all] virtual

Syntax Description

all Display the virtual server IP address of all virtual servers.

Defaults

Omitting the **all** keyword displays the explicitly configured IP address of the current virtual server or servers.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

You must be in privileged EXEC mode to use this command.

Examples

This example displays the **show running-config virtual** command output for a situation in which there is a previously configured HTTP virtual server:

```
hostname(config)# show running-config virtual
virtual http 192.168.201.1
```

Related Commands

Command	Description
clear configure virtual	Removes virtual command statements from the configuration.
virtual	Displays the address for authentication virtual servers.

show running-config vpn load-balancing

To display the current VPN load-balancing virtual cluster configuration, use the **show running-config vpn load-balancing** command in global configuration, privileged EXEC or VPN load-balancing mode.

show running-config [all] vpn load-balancing

Syntax Description

all	Display both the default and the explicitly configured VPN load-balancing configuration.
------------	--

Defaults

Omitting the **all** keyword displays the explicitly configured VPN load-balancing configuration.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—
Vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config vpn load-balancing** command also displays configuration information for the following related commands: **cluster encryption**, **cluster ip address**, **cluster key**, **cluster port**, **nat**, **participate**, and **priority**.

Examples

This example displays **show running-config vpn load-balancing** command and its output, with the **all** option enabled:

```
hostname(config)# show running-config all vpn load-balancing
vpn load-balancing
no nat
priority 9
interface lbpublic test
interface lbprivate inside
no cluster ip address
no cluster encryption
cluster port 9023
no participate
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes vpn load-balancing command statements from the configuration.
show vpn load-balancing	Displays the VPN load-balancing runtime statistics.
vpn load-balancing	Enters vpn load-balancing mode.

show running-config webvpn

To display the running configuration for webvpn, use the **show running-config webvpn** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-config [all] webvpn [apcf | auto-signon | cache | proxy-bypass | rewrite | sso-server | url-list]

Syntax Description

all	(Optional) Displays the running configuration including default values.
apcf	(Optional) Displays the running configuration for SSL VPN APCF.
auto-signon	(Optional) Displays the running configuration for SSL VPN auto sign-on.
cache	(Optional) Displays the running configuration for SSL VPN caching.
proxy-bypass	(Optional) Displays the running configuration for SSL VPN proxy bypass.
rewrite	(Optional) Displays the running configuration for SSL VPN content transformation.
sso-server	(Optional) Displays the running configuration for single sign-on.
url-list	(Optional) Displays the running configuration for SSL VPN access to URLs.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was revised.

Command Modes

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

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

Examples

The following is sample output from the **show running-config webvpn** command:

```
hostname# show running-configuration webvpn
webvpn
  title WebVPN Services for ASA-4
  title-color green
  default-idle-timeout 0
  nbns-server 10.148.1.28 master timeout 2 retry 2
```



```

accounting-server-group RadiusACS1
authentication-server-group RadiusACS2
authorization-dn-attributes CN

```

The following is sample output from the **show running-config all webvpn** command:

```

hostname#(config-webvpn)# show running-config all webvpn

webvpn
title WebVPN Services for ASA-4
username-prompt Username
password-prompt Password
login-message Please enter your username and password
logout-message Goodbye
no logo
title-color green
secondary-color #CCCCFF
text-color white
secondary-text-color black
default-idle-timeout 0
no http-proxy
no https-proxy
nbns-server 10.148.1.28 master timeout 2 retry 2
accounting-server-group RadiusACS1
authentication-server-group RadiusACS2
no authorization-server-group
default-group-policy DfltGrpPolicy
authentication aaa
no authorization-required
authorization-dn-attributes CN
hostname#

```

The following is sample output from the **show running-config webvpn sso-server** command:

```

hostname#(config-webvpn)# show running-config webvpn sso-server
sso-server
sso-server bxbsvr type siteminder
web-agent-url http://bxb-netegrity.demo.com/vpnauth/
policy-server-secret cisco1234
sso-server policysvr type siteminder
web-agent-url http://webagent1.mysiteminder.com/ciscoauth/
policy-server-secret Cisco1234
max-retry-attempts 4
request-timeout 10
hostname#(config-webvpn)#

```

Related Commands

Command	Description
clear configure webvpn	Removes all nondefault SSL VPN configuration attributes.
debug webvpn	Displays debug information about SSL VPN sessions.
show webvpn	Displays statistics about SSL VPN sessions.

show running-config webvpn auto-signon

To display all WebVPN auto-signon assignments in the running configuration, use the **show running-config webvpn auto-signon** command in global configuration mode.

show running-config webvpn auto-signon

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:

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

Release	Modification
7.1(1)	This command was introduced.

Examples The following is sample output from the **show running-config webvpn auto-signon**:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
hostname(config-webvpn)# auto-signon allow uri *.example.com/* auth-type basic
hostname(config-webvpn)# show running-config webvpn auto-signon
auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
auto-signon allow uri *.example.com/* auth-type basic
```

Related Commands	auto-signon	Configures the ASA to automatically pass WebVPN login credentials to internal servers.
-------------------------	--------------------	--

show running-config zonelabs-integrity

To display the Zone Labs Integrity Server configuration, use the **show running-config zonelabs-integrity** command in privileged EXEC mode.

show running-config [all] zonelabs-integrity

Syntax Description

all (Optional) Shows the running configuration including default configuration values.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command to display the addresses of all Zone Labs Integrity Servers and the configured values for the active Zone Labs Integrity Server. Use the **all** parameter to display the default as well as the explicitly configured values.


Examples

The following is sample output from the **show running-config zonelabs-integrity** command:

```
hostname# show running-config zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
hostname#
```

The following is sample output from the **show running-config all zonelabs-integrity** command:

```
hostname# show running-config all zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
zonelabs-integrity interface none
zonelabs-integrity fail-open
zonelabs-integrity fail-timeout 10
zonelabs-integrity ssl-client-authentication disable
zonelabs-integrity ssl-certificate-port 80
hostname#
```

 show running-config zonelabs-integrity

Related Commands	Command	Description
	clear configure zonelabs-integrity	Clears the Zone Labs Integrity Server configuration.

show running-config vpdn

To display the VPDN configuration used for PPPoE connections, use the **show running-config vpdn** command in privileged EXEC mode:

show running-config vpdn

Syntax Description This command has no arguments or keywords.

Defaults This command has no default behavior or values.

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

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

Release	Modification
7.2(1)	This command was introduced.

Examples This following is sample output from the **show running-config vpdn** command:

```
hostname# show running-config vpdn
vpdn group telecommuters ppp authentication mschap
vpdn username tomm password ***** store-local
```

Command	Description
show running-config vpdn group	Shows the current configuration for the VPDN group.
show running-config vpdn username	Shows the current configuration for vpdn usernames.

show running-configuration vpn-sessiondb

To display the current set of configured vpn-sessiondb commands, use the **show running-configuration vpn-sessiondb** command in privileged EXEC mode.

show running-configuration [all] vpn-sessiondb

Syntax Description

all (Optional) Displays all **vpn-sessiondb** commands, including the commands you have not changed from the default

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

As of Release 7.0, this command displays only the VPN maximum sessions limit, if configured.

Examples

The following is sample output for the **show running-configuration vpn-sessiondb** command:

```
hostname# show running-configuration vpn-sessiondb
```

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions

show running-config wccp

To show the WCCP configuration in the running configuration, use the **show running-config wccp** command in privileged EXEC mode.

show [all] running-config wccp

Syntax	Description
all	Displays the default and explicitly configured configuration information for one or all WCCP commands.

Defaults This command has no arguments or keywords.

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

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

Command History	Release	Modification
	7.2(1)	This command was introduced.

Examples The following is sample output from the **show running-config wccp** command:

```
hostname# show running-config wccp
wccp web-cache redirect-list wooster group-list jeeves password whatho
hostname#
```

Related Commands	Command	Description
	wccp	Enables support of WCCP.
	wccp redirect	Enters support of WCCP redirection.

show running-config xlate

To show the **xlate per-session** rules, use the **show running-config xlate** command in global configuration mode.

show running-config [all] xlate

Syntax Description

all (Optional) Shows the running configuration, including default configuration values.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

Use the **clear configure xlate** command to clear the **xlate per-session** configuration.

Examples

The following is sample output from the **show running-config xlate** and **show running-config all xlate** commands:

```
hostname(config)# show running-config xlate
hostname(config)# show running-config all xlate
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

Related Commands

Command	Description
clear configure xlate	Clears the xlate per-session rules.
nat (global)	Adds a twice NAT rule.

Command	Description
nat (object)	Adds an object NAT rule.
xlate per-session	Adds a per-session PAT rule.

