Command Reference

This appendix describes the SSL Services Module commands.

Table A-1 provides a brief description of the commands contained in this appendix.

Table A-1 Command Descriptions

Command	Description
clear ssl-proxy connection	Clears the SSL connections.
clear ssl-proxy stats	Resets the statistics counters maintained in different SSL Services Module system components.
crypto ca import	Imports a PKCS12 file to the SSL Services Module.
crypto ca export	Exports a PKCS12 file from the SSL Services Module.
debug ssl-proxy	Turns on the debug flags in different system components.
show ssl-proxy admin-info	Displays the administration VLAN and related IP and gateway addresses.
show ssl-proxy buffers	Displays the TCP buffer usage information.
show ssl-proxy certificate-history	Displays the certificate event history information.
show ssl-proxy conn	Displays the TCP connections from the SSL Services Module.
show ssl-proxy crash-info	Displays the crash information.
show ssl-proxy mac address	Displays the current MAC address.
show ssl-proxy natpool	Displays NAT pool information.
show ssl-proxy policy	Displays the configured SSL or TCP policies.
show ssl-proxy service	Displays the configured SSL virtual server information.
show ssl-proxy stats	Displays statistics counter information.
show ssl-proxy status	Displays status information.
show ssl-proxy version	Displays the current image version.
show ssl-proxy vlan	Displays VLAN information.
ssl-proxy crypto selftest	Initiates a cryptographic self-test.
ssl-proxy mac address	Configures a MAC address.

Table A-1 Command Descriptions (continued)

Command	Description
ssl-proxy natpool	Defines a pool of IP addresses that the SSL module uses for implementing the client NAT.
ssl-proxy pki history	Enables the public key infrastruture (PKI) event history option.
ssl-proxy policy ssl	Enters the SSL-policy configuration submode where you can define the SSL of a TCP policy for one or more SSL proxy services.
ssl-proxy policy tcp	Enters the proxy-policy TCP configuration submode where you can define the TCP policy templates.
ssl-proxy service	Enters the proxy-service configuration submode where you can configure the virtual IP address and port associated with the proxy service and the associated target IP address and port. You can also define TCP and SSL policies for both the client side and the server side of the proxy.
ssl-proxy ssl ratelimit	Prohibits new connections during overload conditions.
ssl-proxy vlan	Enters the proxy VLAN configuration submode where you can configure a VLAN for the SSL Services Module.

Table A-2 lists the modes and submode commands.

Table A-2 Commands and Submode Commands

Commands	Submode Commands
ssl-proxy policy ssl	**cipher** {**rsa-with-3des-ede-cbc-sha** | **rsa-with-des-cbc-sha** | **rsa-with-rc4-128-md5** | **rsa-with-rc4-128-sha** | **all**}
	[**no**] **close-protocol**
	default {**cipher** | **close-protocol** | **session-cache** | **version**}
	exit
	help
	[**no**] **session-cache**
	[**no**] **timeout handshake** *time*
	version {**all** | **ssl3** | **tls1**}
ssl-proxy policy tcp	**exit**
	[**no**] **timeout fin-wait** *timeout-in-seconds*
	help
	[**no**] **timeout inactivity** *timeout-in-seconds*
	[**no**] **buffer-share rx** *buffer-limit-in-bytes*
	[**no**] **buffer-share tx** *buffer-limit-in-bytes*
	[**no**] **mss** *max-segment-size-in-bytes*
	[**no**] **timeout syn** t*imeout-in-seconds*

Table A-2 Commands and Submode Commands (continued)

Commands	Submode Commands
ssl-proxy service	**certificate rsa general-purpose trustpoint** *trustpoint-name*
	default {**nat**}
	exit
	help
	inservice
	nat {**server** | **client** *natpool-name*}
	server ipaddr *ip-addr* **protocol** *protocol* **port** *portno*
	server policy tcp *server-side-tcp-policy-name*
	virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]
	virtual {**policy ssl** *ssl-policy-name*}
	virtual {**policy tcp** *client-side-tcp-policy-name*}
ssl-proxy vlan	**admin**
	exit
	gateway *prefix* [**drop** | **forward**]
	help
	ipaddr *prefix mask*
	no
	route {*prefix mask*} {**gateway** *prefix*}

clear ssl-proxy connection

To clear all TCP connections on the entire system, use the **clear ssl-proxy connection** command.

clear ssl-proxy connection

Syntax Description

service *name*	(Optional) Clears the connections for the specified service.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To reset all the statistics counters that the SSL Services Module maintained, use the **clear ssl-proxy connection** command without options.

Examples

This example shows how to clear the connections for the specified service:

```
ssl-proxy# clear ssl-proxy connection service S6
```

This example shows how to clear all TCP connections on the entire system:

```
ssl-proxy# clear ssl-proxy connection
ssl-proxy#
```

clear ssl-proxy stats

To reset the statistics counters maintained in different SSL Services Module system components, use the **clear ssl-proxy stats** command.

clear ssl-proxy stats [**crypto** | **fdu** | **ipc** | **pki** | **service** | **ssl** | **tcp**]

Syntax Description

crypto	(Optional) Clears the crypto statistics information.
fdu	(Optional) Clears the F6DU statistics information
ipc	(Optional) Clears the IPC statistics information.
pki	(Optional) Clears the public key infrastruture (PKI) statistics information.
service *name*	(Optional) Clears the statistics information for a specific service.
ssl	(Optional) Clears the SSL statistics information
tcp	(Optional) Clears the TCP statistics information

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To reset all the statistics counters that the SSL Services Module maintained, use the **clear ssl-proxy stats** command without options.

Examples

These examples show how to reset the statistics counters maintained in different system components on the SSL Services Module:

```
ssl-proxy# clear ssl-proxy stats crypto
ssl-proxy# clear ssl-proxy stats ipc
ssl-proxy# clear ssl-proxy stats pki
ssl-proxy# clear ssl-proxy stats service S6
```

This example shows how to clear all statistic counters that the SSL Services Module maintained:

```
ssl-proxy# clear ssl-proxy stats
ssl-proxy#
```

crypto ca import

To import a PKCS12 file to the SSL Services Module, use the **crypto ca import** command.

crypto ca import *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

Syntax Description

trustpoint_label	Specifies the trustpoint label.
file_system	Specifies the file system. Valid values are **scp:**, **ftp:**, **nvram:**, **rcp:**, and **tftp:**
pkcs12_filename	Specifies the name of the PKCS12 file to import.
pass_phrase	Specifies the pass phrase of the PKCS12 file.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

If you are using SSH, we recommend using SCP (secure file transfer) when importing a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify *pkcs12_filename*, you will be prompted to accept the default filename (the default filename is the *trustpoint_label*) or to enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename*.

You will receive an error if you enter the pass phrase incorrectly.

Examples

This example shows how to import a PKCS12 file using SCP:

```
ssl-proxy(config)# crypto ca import TP2 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Source username [ssl-proxy]? admin-1
Source filename [TP2]? /users/admin-1/pkcs12/TP2.p12

Password:password
Sending file modes:C0644 4379 TP2.p12
!
ssl-proxy(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
ssl-proxy(config)#
```

crypto ca export

To export a PKCS12 file from the SSL Services Module, use the **crypto ca export** command.

crypto ca export *trustpoint_label* **pkcs12** *file_system* [*pkcs12_filename*] *pass_phrase*

Syntax Description

trustpoint_label	Specifies the trustpoint label.
file_system	Specifies the file system. Valid values are **scp:, ftp:, nvram:, rcp:,** and **tftp:**
pkcs12_filename	Specifies the name of the PKCS12 file to import.
pass_phrase	Specifies the pass phrase of the PKCS12 file.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Imported key pairs cannot be exported.

If you are using SSH, we recommend using SCP (secure file transfer) when exporting a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify *pkcs12_filename*, you will be prompted to accept the default filename (the default filename is the *trustpoint_label*) or enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename*.

You will receive an error if you enter the pass phrase incorrectly.

Examples

This example shows how to export a PKCS12 file using SCP:

```
ssl-proxy(config)#crypto ca export TP1 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination username [ssl-proxy]? admin-1
Destination filename [TP1]? TP1.p12

Password:

Writing TP1.p12 Writing pkcs12 file to scp://admin-1@10.1.1.1/TP1.p12

Password:
!
CRYPTO_PKI:Exported PKCS12 file successfully.
ssl-proxy(config)#
```

debug ssl-proxy

To turn on the debug flags in different system components, use the **debug ssl-proxy** command. Use the **no** form of this command to turn off the debug flags.

debug ssl-proxy {**app** | **fdu** | **ipc** | **pki** | **ssl** | **tcp**}

Syntax Description

app	Turns on App debugging.
fdu [*type*]	Turns on FDU debugging; (optional) *type* valid values are **cli**, **hash**, **ipc**, and **trace**. See the "Usage Guidelines" section for additional information.
ipc	Turns on IPC debugging.
pki [*type*]	Turns on PKI debugging; (optional) *type* valid values are **cert**, **events**, **history**, **ipc**, and **key**. See the "Usage Guidelines" section for additional information.
ssl [*type*]	Turns on SSL debugging; (optional) *type* valid values are **alert**, **error**, **handshake**, and **pkt**. See the "Usage Guidelines" section for additional information.
tcp [*type*]	Turns on TCP debugging; (optional) *type* valid values are **event**, **packet**, **state**, and **timers**. See the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **fdu** *type* includes the following values:

- **cli**—Debugs the FDU CLI.
- **hash**—Debugs the FDU hash.
- **ipc** —Debugs the FDU IPC.
- **trace**—Debugs the FDU trace.

The **pki** *type* includes the following values:

- **certs**—Debugs the certificate management.
- **events**—Debugs events.
- **history**—Debugs the certificate history.
- **ipc**—Debugs the IPC messages and buffers.
- **key**—Debugs key management.

The **ssl** *type* includes the following values:

- **alert**—Debugs the SSL alert events.
- **error**—Debugs the SSL error events.
- **handshake**—Debugs the SSL handshake events.
- **pkt**—Debugs the received and transmitted SSL packets.

Note Use the TCP debug commands only to troubleshoot basic connectivity issues under little or no load conditions (for instance when no connection is being established to the virtual server or real server).

If you run TCP debug commands, the TCP module displays large amounts of debug information on the console, which can significantly slow down module performance. Slow module performance can lead to delayed processing of TCP connection timers, packets, and state transitions.

The **tcp** *type* includes the following values:

- **events**—Debugs the TCP events.
- **pkt**—Debugs the received and transmitted TCP packets.
- **state**—Debugs the TCP states.
- **timers**—Debugs the TCP timers.

Examples

This example shows how to turn on App debugging:

```
ssl-proxy# debug ssl-proxy app
ssl-proxy#
```

This example shows how to turn on FDU debugging:

```
ssl-proxy# debug ssl-proxy fdu
ssl-proxy#
```

This example shows how to turn on IPC debugging:

```
ssl-proxy# debug ssl-proxy ipc
ssl-proxy#
```

This example shows how to turn on PKI debugging:

```
ssl-proxy# debug ssl-proxy pki
ssl-proxy#
```

This example shows how to turn on SSL debugging:

```
ssl-proxy# debug ssl-proxy ssl
ssl-proxy#
```

This example shows how to turn on TCP debugging:

```
ssl-proxy# debug ssl-proxy tcp
ssl-proxy#
```

This example shows how to turn off TCP debugging:

```
ssl-proxy# no debug ssl-proxy tcp
ssl-proxy#
```

show ssl-proxy admin-info

To display the administration VLAN and related IP and gateway addresses, use the **show ssl-proxy admin-info** command.

show ssl-proxy admin-info

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the administration VLAN and related IP and gateway addresses:

```
ssl-proxy# show ssl-proxy admin-info
STE administration VLAN: 2
STE administration IP address: 207.57.100.18
STE administration gateway: 207.0.207.5
ssl-proxy#
```

Related Commands

ssl-proxy vlan

show ssl-proxy buffers

To display the TCP buffer usage information, use the **show ssl-proxy buffers** command.

show ssl-proxy buffers

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the buffer usage and other information in the TCP subsystem:

```
ssl-proxy# show ssl-proxy buffers
Buffers info for TCP module 1
TCP data buffers used 2816 limit 112640
TCP ingress buffer pool size 56320 egress buffer pool size 56320
TCP ingress data buffers min-thresh 7208960 max-thresh 21626880
TCP ingress data buffers used Current 0 Max 0
TCP ingress buffer RED shift 9 max drop prob 10
Conns consuming ingress data buffers 0
Buffers with App 0
TCP egress data buffers used Current 0 Max 0
Conns consuming egress data buffers 0
In-sequence queue bufs 0 OOO bufs 0
ssl-proxy#
```

Related Commands

ssl-proxy policy tcp

show ssl-proxy certificate-history

To display the certificate event history information, use the **show ssl-proxy certificate-history** command.

show ssl-proxy certificate-history [**service** [*name*]]

Syntax Description

service [*name*]	Displays all certificate records of a proxy service and (optionally) for a specific proxy service.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **show ssl-proxy certificate-history** command displays these records:

- service name
- keypair name
- generation or import time
- trustpoint name
- certificate subject name
- certificate issuer name
- serial number
- date

A syslog message is generated for each record. The oldest records are deleted after the limit of 512 records is reached.

Examples

This example shows how to display the event history of all the certificate processing:

```
ssl-proxy# show ssl-proxy certificate-history
Record 1, Timestamp:00:00:51, 16:36:34 UTC Oct 31 2002
    Installed Server Certificate, Index 5
    Proxy Service:s1,  Trust Point:t3
    Key Pair Name:k3,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:12:27:58 UTC Oct 30 2002
    Subject Name:OID.1.2.840.113549.1.9.2 = simpson5-2-ste.cisco.com,
OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5D3D1931000100000D99
    Validity Start Time:21:58:12 UTC Oct 30 2002
    End Time:22:08:12 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 2, Timestamp:00:01:06, 16:36:49 UTC Oct 31 2002
    Installed Server Certificate, Index 6
    Proxy Service:s5,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
% Total number of certificate history records displayed = 4
ssl-proxy#
```

This example shows how to display the certificate record for a specific proxy service:

```
ssl-proxy# show ssl-proxy certificate-history service s6
Record 3, Timestamp:00:01:34, 16:37:18 UTC Oct 31 2002
    Installed Server Certificate, Index 7
    Proxy Service:s6,  Trust Point:t10
    Key Pair Name:k10,  Key Usage:RSA General Purpose, Exportable
    Time of Key Generation:07:56:43 UTC Oct 11 2002
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.9, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:24BC81B7000100000D85
    Validity Start Time:22:38:00 UTC Oct 19 2002
    End Time:22:48:00 UTC Oct 19 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record

  Record 4, Timestamp:00:01:40, 16:37:23 UTC Oct 31 2002
    Deleted Server Certificate, Index 0
    Proxy Service:s6,  Trust Point:t6
    Key Pair Name:k6,  Key Usage:RSA General Purpose, Not Exportable
    Time of Key Generation:00:28:28 UTC Mar 1 1993
    Subject Name:CN = host1.cisco.com, OID.1.2.840.113549.1.9.2 =
simpson5-2-ste.cisco.com, OID.1.2.840.113549.1.9.8 = 207.79.1.8, OID.2.5.4.5 = B0FFF235
    Issuer Name:CN = SimpsonTestCA, OU = Simpson Lab, O = Cisco Systems, L = San Jose, ST
= CA, C = US, EA =<16> simpson-pki@cisco.com
    Serial Number:5CB5CFD6000100000D97
    Validity Start Time:19:30:26 UTC Oct 30 2002
    End Time:19:40:26 UTC Oct 30 2003
    Renew Time:00:00:00 UTC Jan 1 1970
  End of Certificate Record
Total number of certificate history records displayed = 2
```

Related Commands

ssl-proxy service

show ssl-proxy conn

To display the TCP connections from the SSL Services Module, use the **show ssl-proxy conn** command.

show ssl-proxy conn 4tuple [local {**ip** *local-ip-addr local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [local {**port** *local-port*} [**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]]

show ssl-proxy conn 4tuple [local {**remote** [{**ip** *remote-ip-addr* [**port** *remote-port*]} | {**port** *remote-port* [**ip** *remote-ip-addr*]}]]

show ssl-proxy conn service *name*

Syntax Description

4tuple	Displays the TCP connections for a specific address.
local	(Optional) Displays the TCP connections for a specific local device.
ip *local-ip-addr*	IP address of a local device.
local-port	Port number of a local device.
remote	(Optional) Displays the TCP connections for a specific remote device.
ip *remote-ip-addr*	IP address of a remote device.
port *remote-port*	Port number of a remote device.
port *local-port*	(Optional) Displays the TCP connections for a specific local port.
service *name*	Displays the TCP connections for a specific proxy service.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

These examples show different ways to display the TCP connection established from the SSL Services Module:

```
ssl-proxy# show ssl-proxy conn
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.0.0.10:4430         1.200.200.14:48582    2    0      0      0      ESTAB
1.200.200.14:48582    2.100.100.72:80       2    1      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48583    2    2      0      0      ESTAB
1.200.200.14:48583    2.100.100.72:80       2    3      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48584    2    4      0      0      ESTAB
1.200.200.14:48584    2.100.100.72:80       2    5      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48585    2    6      0      0      ESTAB
1.200.200.14:48585    2.100.100.72:80       2    7      0      0      ESTAB

2.0.0.10:4430         1.200.200.14:48586    2    8      0      0      ESTAB
1.200.200.14:48586    2.100.100.72:80       2    9      0      0      ESTAB

ssl-proxy# show ssl-proxy conn 4tuple local port 443
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.133:443       1.200.200.12:39728    2    113676 0      0      TWAIT
No Bound Connection

2.50.50.133:443       1.200.200.12:39729    2    113680 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:40599    2    113684 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48031    2    114046 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48032    2    114048 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48034    2    114092 0      0      TWAIT
No Bound Connection

2.50.50.132:443       1.200.200.13:48035    2    114100 0      0      TWAIT
No Bound Connection
```

```
ssl-proxy# show ssl-proxy conn 4tuple remote ip 1.200.200.14
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:38814    2    58796  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38815    2    58800  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38817    2    58802  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38818    2    58806  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38819    2    58810  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38820    2    58814  0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:38821    2    58818  0      0      TWAIT
No Bound Connection

ssl-proxy# show ssl-proxy conn service iis1
Connections for TCP module 1
Local Address         Remote Address        VLAN Conid  Send-Q Recv-Q State
--------------------- --------------------- ---- ------ ------ ------ ------
2.50.50.131:443       1.200.200.14:41217    2    121718 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41218    2    121722 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41219    2    121726 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41220    2    121794 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41221    2    121808 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41222    2    121940 0      0      TWAIT
No Bound Connection

2.50.50.131:443       1.200.200.14:41223    2    122048 0      0      TWAIT
No Bound Connection
```

show ssl-proxy crash-info

To collect software-forced reset information on from the SSL Services Module, use the **show ssl-proxy crash-info** command.

show ssl-proxy crash-info

Syntax Description

This command has no arguments or keywords

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

The following example shows how to collect software-forced reset information:

```
ssl-proxy# show ssl-proxy crash-info

===== SSL SERVICE MODULE - START OF CRASHINFO COLLECTION =====


------------- COMPLEX 0 [FDU_IOS] ----------------------

NVRAM CHKSUM:0xB562
NVRAM MAGIC:0xC8A514F0

++++++++++ CORE 0 +++++++++++++++++++++++++++++++++

-> CID:1 (IOS)
-> APPLICATION VERSION:
-> APPROXIMATE TIME:00:00:00 UTC Jan 1 1970
-> GENUINE:3391429263 This core has crashed
-> TRACEBACK:DDBE3FEF 887090E7 222DA8
-> CPU CONTEXT  ----------------------------

$0 :00000000, AT :00000000, v0 :00260000, v1 :37EF9598
a0 :00000001, a1 :00000001, a2 :0000003C, a3 :00233280
t0 :002474C4, t1 :00000004, t2 :00000000, t3 :00000001
t4 :00000010, t5 :00000001, t6 :00000001, t7 :00000001
s0 :00000000, s1 :004C4B3F, s2 :002474CC, s3 :00000000
s4 :00000000, s5 :0000003C, s6 :0000003C, s7 :00000019
t8 :0000000F, t9 :00000000, k0 :00000100, k1 :00400001
gp :00000000, sp :0023AEC0, s8 :031FFF58, ra :00000064
LO :00000000, HI :00000000, BADVADDR :0000000C
EPC :00000000, ErrorEPC :00222DA8, SREG :00000000
```

```
Cause 27299127 (Code 0x9):Breakpoint exception

-> PROCESS STACK -----------------------------
->    stack top:0x0

  Process stack in use ( sp -> stack_top ):

->  sp out of recorded stack area. Stack bottom:0xFFFFC000



0023AEB4:                           00000000              ....
0023AEC4:03200000 02B01021 26440A30 0C197B99  . ...0.!&D.0..{.
0023AED4:90450000 26020001 30420003 14400004  .E..&...0B...@..

............
............
............

FFFFFFD0:00000000 00000000 00000000 00000000  ................
FFFFFFE0:00627E34 00000000 00000000 00000000  .b~4............
FFFFFFF0:00000000 00000000 00000000 00000006  ................
00000000:




===== SSL SERVICE MODULE - END OF CRASHINFO COLLECTION =======
```

show ssl-proxy mac address

To display the current MAC address, use the **show ssl-proxy mac address** command.

show ssl-proxy mac address

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the current MAC address used in the SSL Services Module:

```
ssl-proxy# show ssl-proxy mac address
STE MAC address: 00e0.b0ff.f232
ssl-proxy#
```

show ssl-proxy natpool

To display NAT pool information, use the **show ssl-proxy natpool** command.

show ssl-proxy natpool [*name*]

Syntax Description

name	(Optional) NAT pool name.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display information for a specific NAT address pool configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy natpool NP1
Start ip: 207.57.110.1
End ip: 207.57.110.8
netmask: 255.0.0.0
vlan associated with natpool: 2
SSL proxy services using this natpool:
S2
S3
S1
S6
Num of proxies using this natpool: 4
ssl-proxy#
```

Related Commands

ssl-proxy natpool

show ssl-proxy policy

To display the configured SSL or TCP policies, use the **show ssl-proxy policy** command.

show ssl-proxy policy {**ssl** | **tcp**} [*name*]

Syntax Description

ssl	Displays the configured SSL policies.
tcp	Displays the configured TCP policies.
name	(Optional) Policy name.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display policy information for a specific SSL policy configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy policy ssl ssl-policy1
Cipher suites: (None configured, default ciphers included)
     rsa-with-rc4-128-md5
     rsa-with-rc4-128-sha
     rsa-with-des-cbc-sha
     rsa-with-3des-ede-cbc-sha
SSL Versions enabled:SSL3.0, TLS1.0
strict close protocol:disabled
Session Cache:enabled
Handshake timeout not configured (never times out)
Num of proxies using this poilicy:0
```

This example shows how to display policy information for a specific TCP policy configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy policy tcp tcp-policy1
MSS                  1250
SYN timeout          75
Idle timeout          600
FIN wait timeout     75
Rx Buffer Share  32768
Tx Buffer Share  32768

Usage count of this policy:0
ssl-proxy#
```

show ssl-proxy service

To display the configured SSL virtual server information, use the **show ssl-proxy service** command.

show ssl-proxy service [*name*]

Syntax Description

name	(Optional) Service name.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display all SSL virtual services configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy service

Proxy Service Name Admin Operation Events
status status
S2 up up
S3 up up
S1 up up
S6 down down
ssl-proxy#
```

This example shows how to display a specific SSL virtual service configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy service S6
Service id: 3, bound_service_id: 259
Virtual IP: 207.59.100.20, port: 443
Server IP: 207.50.0.50, port: 80
Virtual TCP Policy: tcppl1
Virtual SSL Policy: sslpl1
Nat pool: NP1
rsa-general-purpose certificate trustpoint: tp1
Certificate chain in use for new connections:
Server Certificate:
Key Label: KEY1
Serial Number: 1AEE011F000100000552
```

```
Root CA Certificate:
Serial Number: 313AD6510D25ABAE4626E96305511AC4
Certificate chain complete
Admin Status: down
Operation Status: down
ssl-proxy#
```

show ssl-proxy stats

To display statistics counter information, use the **show ssl-proxy stats** command.

show ssl-proxy stats [*type*]

Syntax Description

type	(Optional) Information type; valid values are **crypto**, **ipc**, **pki**, **service**, **ssl**, and **tcp**. See the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *type* values are defined as follows:

- **crypto**—Displays crypto statistical information.
- **ipc**—Displays IPC statistical information.
- **pki**—Displays PKI statistical information.
- **service**—Displays proxy service statistical information.
- **ssl**—Displays SSL detailed statistical information.
- **tcp**—Displays TCP detailed statistical information.

Examples

This example shows how to display all the statistics counters collected on the SSL Services Module:

```
ssl-proxy# show ssl-proxy stats
TCP Statistics:
    Conns initiated     :0            Conns accepted      :0
    Conns established   :0            Conns dropped       :0
    Conns closed        :0            SYN timeouts        :0
    Idle timeouts       :0            Total pkts sent     :0
    Data packets sent   :0            Data bytes sent     :0
    Total Pkts rcvd     :0            Pkts rcvd in seq    :0
    Bytes rcvd in seq   :0
```

```
SSL Statistics:
    conns attempted     :0            conns completed     :0
    full handshakes     :0            resumed handshakes  :0
    active conns        :0            active sessions     :0
    renegs attempted    :0            conns in reneg      :0
    handshake failures  :0            data failures       :0
    fatal alerts rcvd   :0            fatal alerts sent   :0
    no-cipher alerts    :0            ver mismatch alerts :0
    no-compress alerts  :0            bad macs received   :0
    pad errors          :0

FDU Statistics:
    IP Frag Drops       :0            Serv_Id Drops       :0
    Conn Id Drops       :0            Checksum Drops      :0
    IOS Congest Drops   :0            IP Version Drops    :0
    Hash Full Drops     :0            Hash Alloc Fails    :0
    Flow Creates        :0            Flow Deletes        :0
    conn_id allocs      :0            conn_id deallocs    :0
    Tagged Drops        :0            Non-Tagged Drops    :0
    Add ipcs            :36           Delete ipcs         :0
    Disable ipcs        :30           Enable ipcs         :0
    Unsolicited ipcs    :0            Duplicate ADD ipcs  :0
    IOS broadcast pkts  :8520         IOS unicast pkts    :46
    IOS total pkts      :8566         Bound Conn Drops    :0
```

This example shows how to display crypto statistical information:

```
ssl-proxy# show ssl-proxy stats crypto
Crypto Statistics from SSL Module:1
  Self-test is running
  Current device index is 1
  Time interval between tests is 1 seconds
  Device 0 statistics:
    Total Number of runs:50
    Runs all passed:1
    Number of timer error:0
    ------------------------------------------------------------
    Test Name                      Passed  Failed  Did-not-run
    ------------------------------------------------------------
      0  Power-on Crypto chip sel    1       0       0
      1  Power-on Crypto chip key    1       0       0
      2  Hash Test Case 1           50       0       0
      3  Hash Test Case 2           50       0       0
      4  Hash Test Case 3           50       0       0
      5  Hash Test Case 4           50       0       0
      6  SSL3 MAC Test Case 1       50       0       0
      7  SSL3 MAC Test Case 2       50       0       0
      8  TLS1 MAC Test Case 1       50       0       0
      9  TLS1 MAC Test Case 2       50       0       0
     10  DES Server Test            50       0       0
     11  DES Encrypt Test 1         50       0       0
     12  DES Decrypt Test 1         50       0       0
     13  DES Encrypt Test 2         50       0       0
     14  DES Decrypt Test 2         50       0       0
     15  ARC4 Test Case 1           50       0       0
     16  ARC4 Test Case 2           50       0       0
     17  ARC4 Test Case 3           50       0       0
     18  ARC4 State Test Case 1     50       0       0
     19  ARC4 State Test Case 2     50       0       0
     20  ARC4 State Test Case 3     50       0       0
     21  ARC4 State Test Case 4     50       0       0
     22  HMAC Test Case 1           50       0       0
     23  HMAC Test Case 2           50       0       0
     24  Random Bytes Generation    50       0       0
```

```
     25  RSA Encrypt/Decrypt Test   50      0      0
     26  Master Secret Generation   50      0      0
     27  Key Material Generation    50      0      0
     28  SSL3 Handshake Hash Test   50      0      0
     29  TLS1 Handshake Hash Test   50      0      0

  Device 1 statistics:
    Total Number of runs:49
    Runs all passed:1
    Number of timer error:0
    ------------------------------------------------------
    Test Name                     Passed  Failed  Did-not-run
    ------------------------------------------------------
      0  Power-on Crypto chip sel    1      0      0
      1  Power-on Crypto chip key    1      0      0
      2  Hash Test Case 1           50      0      0
      3  Hash Test Case 2           50      0      0
      4  Hash Test Case 3           50      0      0
      5  Hash Test Case 4           50      0      0
      6  SSL3 MAC Test Case 1       50      0      0
      7  SSL3 MAC Test Case 2       50      0      0
      8  TLS1 MAC Test Case 1       50      0      0
      9  TLS1 MAC Test Case 2       50      0      0
     10  DES Server Test            50      0      0
     11  DES Encrypt Test 1         50      0      0
     12  DES Decrypt Test 1         50      0      0
     13  DES Encrypt Test 2         50      0      0
     14  DES Decrypt Test 2         50      0      0
     15  ARC4 Test Case 1           50      0      0
     16  ARC4 Test Case 2           50      0      0
     17  ARC4 Test Case 3           50      0      0
     18  ARC4 State Test Case 1     49      0      0
     19  ARC4 State Test Case 2     49      0      0
     20  ARC4 State Test Case 3     49      0      0
     21  ARC4 State Test Case 4     49      0      0
     22  HMAC Test Case 1           49      0      0
     23  HMAC Test Case 2           49      0      0
     24  Random Bytes Generation    49      0      0
     25  RSA Encrypt/Decrypt Test   49      0      0
     26  Master Secret Generation   49      0      0
     27  Key Material Generation    49      0      0
     28  SSL3 Handshake Hash Test   49      0      0
     29  TLS1 Handshake Hash Test   49      0      0

ssl-proxy#
```

This example shows how to display PKI statistical information:

```
ssl-proxy# show ssl-proxy stats pki
PKI Memory Usage Counters:
  Malloc count:47
  Setstring count:8
  Free count:39
  Malloc failed:0
  Ipc alloc count:12
  Ipc free count:18
  Ipc alloc failed:0
PKI IPC Counters:
  Request buffer sent:6
  Request buffer received:0
  Request duplicated:0
  Request send failed:0
  Response buffer sent:0
  Response buffer received:6
```

```
  Response timeout:0
  Response failed:0
  Response with error reported by SSL Processor:0
  Response with no request:0
  Response duplicated:0
  Message type error:0
  Message length error:0
Key Certificate Table Current Usage (cannot be cleared):
  Total number of entries in table:8192
  Entries in use:2
  Free entries:8190
  Complete server entries:1
  Incomplete new/renew server entries:0
  Retiring server entries:0
  Obsolete server entries:0
  Complete intermediate CA cert:0
  Complete root CA cert:1
  Obsolete intermediate CA cert:0
  Obsolete root CA cert:0
PKI Accumulative Counters (cannot be cleared):
  Proxy service trustpoint added:1
  Proxy service trustpoint deleted:0
  Proxy service trustpoint modified:0
  Keypair added:1
  Keypair deleted:0
  Wrong key type:0
  Server certificate added:1
  Server certificate deleted:0
  Server certificate rolled over:0
  Server certificate completed:1
  Intermediate CA certificate added:0
  Intermediate CA certificate deleted:0
  Root CA certificate added:1
  Root CA certificate deleted:0
  Certificate overwritten:0
  No free table entries:0
  Rollover failed:0
  History records written:0
  History records currently kept in memory:0
  History records have been cleared:0 times
```

show ssl-proxy status

To display status information, use the **show ssl-proxy status** command.

show ssl-proxy status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the status on the SSL Services Module:

```
ssl-proxy# show ssl-proxy status
FDU cpu is alive!
FDU cpu utilization:
    % process util   :0             % interrupt util :0
    proc cycles :0x19079AF          int cycles  :0xB002D1
    total cycles:0x14B8E665C377

TCP cpu is alive!
TCP cpu utilization:
    % process util   :0             % interrupt util :0
    proc cycles :0x3FDE65C          int cycles  :0x14E2EE6599
    total cycles:0x14BD70F8EEB8

SSL cpu is alive!
SSL cpu utilization:
    % process util   :0             % interrupt util :0
    proc cycles :0xC98B5            int cycles  :0x49022586
    total cycles:0x14BD777CE150
```

show ssl-proxy version

To display the current image version, use the **show ssl-proxy version** command.

show ssl-proxy version

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the image version currently running on the SSL Services Module:

```
ssl-proxy# show ssl-proxy version

Cisco Internetwork Operating System Software
IOS (tm) SVCSSL Software (SVCSSL-K9Y9-M), Version 12.2(14.6)SSL(0.19) INTERIM TEST
SOFTWARE
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Thu 10-Apr-03 03:03 by integ
Image text-base: 0x00400078, data-base: 0x00ABE000
ROM: System Bootstrap, Version 12.2(11)YS1 RELEASE SOFTWARE
ssl-proxy uptime is 3 days, 22 hours, 22 minutes
System returned to ROM by power-on
System image file is "tftp://10.1.1.1/unknown"
AP Version 1.1(1)
ssl-proxy#
```

show ssl-proxy vlan

To display VLAN information, use the **show ssl-proxy vlan** command.

show ssl-proxy vlan [*vlan-id* | **debug**]

Syntax Description

vlan-id	(Optional) VLAN ID. Displays information for a specific VLAN; valid values are from 1 to 1005.
debug	(Optional) Displays debug information.

Defaults

This command has no default settings.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display all the VLANs configured on the SSL Services Module:

```
ssl-proxy# show ssl-proxy vlan
VLAN index 2 (admin VLAN)
   IP addr 207.57.100.18 NetMask 255.0.0.0 Gateway 207.0.207.5
   Network 209.0.0.0 Mask 255.0.0.0 Gateway 207.0.207.6
VLAN index 3
   IP addr 208.57.0.18 NetMask 255.0.0.0 Gateway 208.0.207.6
VLAN index 6
   IP addr 209.59.100.18 NetMask 255.0.0.0

ssl-proxy#
```

Related Commands

ssl-proxy vlan

ssl-proxy crypto selftest

To initiate a cryptographic self-test, use the **ssl-proxy crypto selftest** command. Use the **no** form of this command to disable the testing.

ssl-proxy crypto selftest [**time-interval** *seconds*]

no ssl-proxy crypto selftest

Syntax Description

time-interval *seconds*	(Optional) Sets the time interval between test cases; valid values are from 1 to 8 seconds.

Defaults

3 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **ssl-proxy crypto selftest** command enables a set of crypto algorithm tests to be run on the SSL processor in the background. Random number generation, hashing, encryption and decryption, and MAC generation are tested with a time interval in between test cases.

This test is run only for troubleshooting purposes. Running this test will impact run-time performance.

To display the results of the self-test, enter the **show ssl-proxy stats crypto** command.

Examples

This example shows how to start a cryptographic self-test:

```
ssl-proxy (config)# ssl-proxy crypto selftest
ssl-proxy (config)#
```

ssl-proxy mac address

To configure a MAC address, use the **ssl-proxy mac address** command.

ssl-proxy mac address *mac-addr*

Syntax Description

mac-addr	MAC address; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Enter the MAC address in this format: H.H.H.

Examples

This example shows how to configure a MAC address:

```
ssl-proxy (config)# ssl-proxy mac address 00e0.b0ff.f232
ssl-proxy (config)#
```

Related Commands

show ssl-proxy mac address

ssl-proxy natpool

To define a pool of IP addresses which the SSL Services Module uses for implementing the client NAT, use the **ssl-proxy natpool** command.

ssl-proxy natpool *nat-pool-name start-ip-addr* {**netmask** *netmask*}

Syntax Description

nat-pool-name	NAT pool name.
start-ip-addr	Start IP address.
netmask *netmask*	Netmask; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to define a pool of IP addresses:

```
ssl-proxy (config)# ssl-proxy natpool NP2 207.59.10.01 207.59.10.08 netmask 255.0.0.0
ssl-proxy (config)#
```

Related Commands

show ssl-proxy natpool

ssl-proxy pki history

To enable the PKI event history option, use the **ssl-proxy pki history** command. Use the **no** form of this command to disable the logging and clear the memory.

ssl-proxy pki history

no ssl-proxy pki history

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **ssl-proxy pki history** command enables logging of certificate history records per-proxy service into memory and generates a syslog message per record. Each record keeps track of the addition or deletion of a keypair or certificate into the proxy services key and the certificate table.

When the index of the table changes, this command logs the following information:

- Key pair name
- Trustpoint label
- Service name
- Subject name
- Serial number of the certificate

Up to 512 records can be stored in the memory at one time.

Examples

This example shows how to enable the PKI event history option:

```
ssl-proxy (config)# ssl-proxy pki history
ssl-proxy (config)#
```

Related Commands

show ssl-proxy stats

ssl-proxy policy ssl

To enter the SSL policy configuration submode, use the **ssl-proxy policy ssl** command. In the SSL policy configuration submode, you can define the TCP policy for one or more SSL proxy services.

ssl-proxy policy ssl *ssl-policy-name*

Syntax Description

ssl-policy-name	SSL policy name.

Defaults

The defaults are as follows:

- **cipher** is **all**
- **close-protocol strict** is disabled
- **session-cache** is enabled
- **timeout** is **0**
- **version** is **all**

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Each SSL policy configuration submode command is entered on its own line.

Table A-3 lists the commands available in SSL policy configuration submode.

Table A-3 SSL Policy Configuration Submode Command Descriptions

cipher {**rsa-with-3des-ede-cbc-sha** | **rsa-with-des-cbc-sha** | **rsa-with-rc4-128-md5** | **rsa-with-rc4-128-sha** | **all**}	Allows you to configure a list of cipher-suites acceptable to the proxy server.
[**no**] **close-protocol strict**	Allows you to configure the SSL close protocol behavior. Use the **no** form of this command to disable close-protocol.
default {**cipher** | **close-protocol** | **session-cache** | **version**}	Sets a command to its default settings.
exit	Exits from SSL policy configuration submode.
help	Provides a description of the interactive help system.

Table A-3 SSL Policy Configuration Submode Command Descriptions (continued)

[**no**] **session-cache**	Allows you to enable the session-caching feature. Use the **no** form of this command to disable session caching.
[**no**] **timeout** *time*	Allows you to set how long the SSL services module can keep the connection in handshake phase; valid values are from 0 to 65535 seconds. Use the **no** form of this command to return to the default setting.
version {**all** | **ssl3** | **tls1**}	Allows you to set the version of SSL used to one of the following: • **all**—Both SSL3 and TLS1 versions are used. • **ssl3**—SSL version 3 is used. • **tls1**—TLS version 1 is used.

You can define the SSL policy templates using the **ssl-proxy policy ssl** *ssl-policy-name* command and associate a SSL policy with a particular proxy server using the proxy server configuration CLI. The SSL policy template allows you to define various parameters associated with the SSL handshake stack.

When enabled, a close-notify alert message is sent to the client, and a close-notify alert message also is expected from the client. When disabled, the server sends a close-notify alert message to the client, however, the server does not expect a close-notify alert message from the client; the server waits for a close-notify message before closing the session.

To configure sesssion-cache size, see the **ssl-proxy** global configuration command.

The cipher suite names follow the same convention as the existing SSL stacks.

The cipher suites acceptable to the proxy-server are as follows:

- rsa-with-3des-ede-cbc-sha— RSA with 3des-sha
- rsa-with-des-cbc-sha—RSA with des-sha
- rsa-with-rc4-128-md5—RSA with rc4-md5
- rsa-with-rc4-128-sha—RSA with rc4-sha
- all—All supported ciphers

Setting the handshake timeout to **0** keeps the connection open even if the connection is in handshake mode for an extended period of time.

Examples

This example shows how to enter the SSL policy configuration submode:

```
ssl-proxy (config)# ssl-proxy policy ssl sslpl1
ssl-proxy (config-ssl-policy)#
```

This example shows how to define the cipher suites supported for the SSL policy:

```
ssl-proxy (config-ssl-policy)# cipher rsa-with-3des-ede-cbc-sha
ssl-proxy (config-ssl-policy)#
```

This example shows how to enable the SSL session closing protocol:

```
ssl-proxy (config-ssl-policy)# close-protocol strict
ssl-proxy (config-ssl-policy)#
```

This example shows how to disable the SSL session closing protocol:

```
ssl-proxy (config-ssl-policy)# no close-protocol
ssl-proxy (config-ssl-policy)#
```

These examples show how to set a given command to its default setting:

```
ssl-proxy (config-ssl-policy)# default cipher
ssl-proxy (config-ssl-policy)# default close-protocol
ssl-proxy (config-ssl-policy)# default session-cache
ssl-proxy (config-ssl-policy)# default version
ssl-proxy (config-ssl-policy)#
```

This example shows how to enable the the session-cache option:

```
ssl-proxy (config-ssl-policy)# session-cache
ssl-proxy (config-ssl-policy)#
```

This example shows how to disable the the session-cache option:

```
ssl-proxy (config-ssl-policy)# no session-cache
ssl-proxy (config-ssl-policy)#
```

This example shows how to set how long the SSL Services Module can keep the connection in handshake phase:

```
ssl-proxy (config-ssl-policy)# timeout 20
ssl-proxy (config-ssl-policy)#
```

These examples show how to enable the support of different SSL versions:

```
ssl-proxy (config-ssl-policy)# all
ssl-proxy (config-ssl-policy)# ssl3
ssl-proxy (config-ssl-policy)# tls1
ssl-proxy (config-ssl-policy)#
```

This example shows how to print out a general help page:

```
ssl-proxy (config-ssl-policy)# help
ssl-proxy (config-ssl-policy)#
```

Related Commands show ssl-proxy policy

ssl-proxy policy tcp

To enter the proxy policy TCP configuration submode, use the **ssl-proxy policy tcp** command. In proxy policy TCP configuration submode, you can define the TCP policy templates.

ssl-proxy policy tcp *tcp-policy-name*

Syntax Description

tcp-policy-name	TCP policy name.

Defaults

The defaults are as follows:

- **timeout inactivity** is 240 seconds
- **timeout fin-wait** is 600 seconds
- **buffer-share rx** is 32768 bytes
- **buffer-share tx** is 32768 bytes
- **mss** is 1500 bytes
- **timeout syn** is 75 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

After you have defined the TCP policy, you can associate the TCP policy with a proxy server using the proxy-policy TCP configuration submode commands.

Each proxy-policy TCP configuration submode command is entered on its own line.

Table A-4 lists the commands available in proxy-policy TCP configuration submode.

Table A-4 Proxy-policy TCP Configuration Submode Command Descriptions

default	Sets a command to its default settings.
exit	Exits from proxy-service configuration submode.
[**no**] **timeout fin-wait** *timeout-in-seconds*	Allows you to configure the FIN wait timeout; vaid values are from 75 to 600 seconds. Use the **no** form of this command to return to the default setting.
help	Provides a description of the interactive help system.

Table A-4 Proxy-policy TCP Configuration Submode Command Descriptions (continued)

[**no**] **timeout inactivity** *timeout-in-seconds*	Allows you to configure the inactivity timeout; valid values are from 0 to 960 seconds. This allows you to set the aging timeout for an idle connection and helps protect the connection resources. Use the **no** form of this command to return to the default setting.
[**no**] **buffer-share rx** *buffer-limit-in-bytes*	Allows you to configure maximum size of the receive buffer share per connection; valid values are from 8192 to 262144. Use the **no** form of this command to return to the default setting.
[**no**] **buffer-share tx** *buffer-limit-in-bytes*	Allows you to configure maximum size of the transmit buffer share per connection; valid values are from 8192 to 262144. Use the **no** form of this command to return to the default setting.
[**no**] **mss** *max-segment-size-in-bytes*	Allows you to configure the maximum segment size the connection identifies in the generated SYN packet; valid values are from 64 to 1460. Use the **no** form of this command to return to the default setting.
[**no**] **timeout syn** *timeout-in-seconds*	Allows you to configure the connection establishment timeout; vaid values are from 5 to 75 seconds. Use the **no** form of this command to return to the default setting.

Usage Guidelines

TCP commands entered on the SSL Services Module can apply either globally or to a particular proxy server.

You can configure a different maximum segment size for the client side and the server side of the proxy server.

The TCP policy template allows you to define parameters associated with the TCP stack.

You can either enter the **no** form of the command to return to the default setting or use the **default** option.

Examples

This example shows how to enter the proxy-policy TCP configuration submode:

```
ssl-proxy (config)# ssl-proxy policy tcp tcppl1
ssl-proxy (config-tcp-policy)#
```

These examples show how to set a given command to its default value:

```
ssl-proxy (config-tcp-policy)# default timeout fin-wait
ssl-proxy (config-tcp-policy)# default inactivity-timeout
ssl-proxy (config-tcp-policy)# default buffer-share rx
ssl-proxy (config-tcp-policy)# default buffer-share tx
ssl-proxy (config-tcp-policy)# default mss
ssl-proxy (config-tcp-policy)# default timeout syn
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the FIN wait timeout in seconds:

```
ssl-proxy (config-tcp-policy)# timeout fin-wait 200
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the inactivity timeout in seconds:

```
ssl-proxy (config-tcp-policy)# timeout inactivity 300
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum receive buffer size configuration:

```
ssl-proxy (config-tcp-policy)# buffer-share rx 16384
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum transmit buffer size configuration:

```
ssl-proxy (config-tcp-policy)# buffer-share tx 13444
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the maximum segment size for TCP:

```
ssl-proxy (config-tcp-policy)# mss 1460
ssl-proxy (config-tcp-policy)#
```

This example shows how to define the initial connection (SYN) timeout value:

```
ssl-proxy (config-tcp-policy)# timeout syn 5
ssl-proxy (config-tcp-policy)#
```

Related Commands show ssl-proxy policy

ssl-proxy service

To enter the proxy-service configuration submode, use the **ssl-proxy-service** command. In proxy-service configuration submode, you can configure the virtual IP address and port associated with the proxy service and the associated target IP address and port. You can also define TCP and SSL policies for both the client side (beginning with the virtual keyword) and the serve side of the proxy (beginning with the **server** keyword).

ssl-proxy service *ssl-proxy-name*

Syntax Description

ssl-proxy-name	SSL proxy name.

Defaults

Server NAT is enabled, and client NAT is disabled

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Each proxy-service configuration submode command is entered on its own line.

Table A-5 lists the commands available in proxy-service configuration submode.

Table A-5 Proxy-service Configuration Submode Command Descriptions

Syntax	Description
certificate rsa general-purpose trustpoint *trustpoint-name*	Configures the certificate with RSA general purpose keys and associates a trustpoint to the certificate.
default {**certificate** | **inservice** | **nat** | **server** | **virtual**}	Sets a command to its default settings.
exit	Exits from ssl-proxy service configuration submode.
help	Provides a description of the interactive help system.
inservice	Declares a proxy server as administratively up.
nat {server | client *natpool-name*}	Specifies the usage of either server NAT or client NAT for the server side connection opened by STE.
server ipaddr *ip-addr* **protocol** *protocol* **port** *portno*	Defines the IP address of the target server for the proxy server. You can also specify the port number and the transport protocol. The target IP address can be a virtual IP address of an SLB device or a real IP address of a web server.

Table A-5 Proxy-service Configuration Submode Command Descriptions (continued)

Syntax	Description
server policy tcp *server-side-tcp-policy-name*	Applies a TCP policy to the server side of a proxy server. You can specify the port number and the transport protocol as well.
virtual {**ipaddr** *ip-addr*} {**protocol** *protocol*} {**port** *portno*} [**secondary**]	Defines the virtual IP address of the virtual server that STE is proxying for. You can also specify the port number and the transport protocol. Valid value for *protocol* is **tcp**; valid values for *portno* is from 1 to 65535. The (optional) **secondary** option prevents the STE from replying to the ARP request coming to the virtual IP address.
virtual {**policy ssl** *ssl-policy-name*}	Applies an SSL policy with the client side of a proxy server.
virtual {**policy tcp** *client-side-tcp-policy-name*}	Applies a TCP policy to the client side of a proxy server.

Both secured and unsecured mode between the CSM and the STE is supported.

Use the (optional) **secondary** option for unsecured topology.

Examples

This example shows how to enter the proxy-service configuration submode:

```
ssl-proxy (config)# ssl-proxy service S6
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the certificate for the specified SSL proxy services:

```
ssl-proxy (config-ssl-proxy)# certificate rsa general-purpose trustpoint tp1
ssl-proxy (config-ssl-proxy)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-ssl-proxy)# default certificate
ssl-proxy (config-ssl-proxy)# default inservice
ssl-proxy (config-ssl-proxy)# default nat
ssl-proxy (config-ssl-proxy)# default server
ssl-proxy (config-ssl-proxy)# default virtual
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a virtual IP address for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual ipaddr 207.59.100.20 protocol tcp port 443
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the SSL policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy ssl sslpl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure the TCP policy for the specified virtual server:

```
ssl-proxy (config-ssl-proxy)# virtual policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a clear-text web server for the SSL Services Module to forward the decrypted traffic:

```
ssl-proxy (config-ssl-proxy)# server ipaddr 207.50.0.50 protocol tcp port 80
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a TCP policy for the given clear-text web server:

```
ssl-proxy (config-ssl-proxy)# server policy tcp tcppl1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to configure a NAT pool for the client address used in the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat client NP1
ssl-proxy (config-ssl-proxy)#
```

This example shows how to enable a NAT server address for the server connection of the specified service SSL offload:

```
ssl-proxy (config-ssl-proxy)# nat server
ssl-proxy (config-ssl-proxy)#
```

Related Commands show ssl-proxy service

ssl-proxy ssl ratelimit

To prohibit new connections during overload conditions, use the **ssl-proxyy ssl ratelimit** command. Use the **no** form of this command to allow new connections as long as memory is available.

ssl-proxyy ssl ratelimit

no ssl-proxyy ssl ratelimit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to prohibit new connections during overload conditions:

```
ssl-proxy (config)# ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

This example shows how to allow new connections during overload conditions as long as memory is available:

```
ssl-proxy (config)# no ssl-proxy ssl ratelimit
ssl-proxy (config)#
```

ssl-proxy vlan

To enter the proxy-VLAN configuration submode, use the **ssl-proxy vlan** command. In proxy-VLAN configuration submode, you can configure a VLAN for the SSL Services Module.

ssl-proxy vlan *vlan*

Syntax Description

vlan	VLAN ID; valid values are from 1 to 1005.

Defaults

This command has no default settings.

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS Release 12.1(13)E and SSL Services Module Release 1.1(1)	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

VLAN 1 is not supported by the CSM.

Extended range VLANs are not supported by the SSL Services Module.

Each proxy-VLAN configuration submode command is entered on its own line.

Table A-6 lists the commands available in proxy-VLAN configuration submode.

Table A-6 Proxy-service Configuration Submode Command Descriptions

Syntax	Description
admin	Configures the VLAN to be an administration VLAN.
exit	Exits from the proxy-VLAN configuration submode.
gateway *prefix* [**drop** | **forward**]	Configures the VLAN with a gateway to the Internet.
help	Provides a description of the interactive help system.
ipaddr *prefix mask*	Configures the VLAN with an IP address and a subnet mask.
no	Negates a command or set its defaults.
route {*prefix mask*} {**gateway** *prefix*}	Configures a gateway for the SSL Services Module to reach a nondirect connected subnetwork.

You must remove the administration VLAN status of the current administration VLAN before you can configure a different administration VLAN.

An administration VLAN is used for communication with the certificate agent (PKI) and the management station (SNMP).

When configuring the gateway, the **drop** option allows the SSL Services Module to drop a packet if a virtual service cannot be found relating to the packet.

When configuring the gateway, the **forward** option allows the SSL Services Module to forward a packet to the gateway of the specified VLAN, if a virtual service cannot be found relating to the packet.

Examples

This example shows how to enter the proxy-VLAN configuration submode:

```
ssl-proxy (config)# ssl-proxy vlan 6
ssl-proxy (config-vlan)#
```

These examples show how to set a specified command to its default value:

```
ssl-proxy (config-vlan)# default admin
ssl-proxy (config-vlan)# default gateway
ssl-proxy (config-vlan)# default ipaddr
ssl-proxy (config-vlan)# default route
```

This example shows how to configure the specified VLAN with a gateway:

```
ssl-proxy (config-vlan)# gateway 209.0.207.5
ssl-proxy (config-vlan)#
```

This example shows how to configure the specified VLAN with an IP address and subnet mask:

```
ssl-proxy (config-vlan)# ipaddr 208.59.100.18 255.0.0.0
ssl-proxy (config-vlan)#
```

This example shows how to configure a gateway for the SSL Services Module to reach a nondirect connected subnetwork:

```
ssl-proxy (config-vlan)# route 210.0.207.0 255.0.0.0 gateway 209.0.207.6
ssl-proxy (config-vlan)#
```

Related Commands

show ssl-proxy vlan