

keepalive (isakmp profile)

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **keepalive** command in Internet Security Association Key Management Protocol (ISAKMP) profile configuration mode. To return to the default, use the **no** form of this command.

keepalive *seconds* **retry** *retry-seconds*

no keepalive *seconds* **retry** *retry-seconds*

Syntax Description

<i>seconds</i>	Number of seconds between DPD messages. The range is from 10 to 3600 seconds.
retry <i>retry-seconds</i>	Number of seconds between retries if DPD message fails. The range is from 2 to 60 seconds.

Defaults

If this command is not configured, a DPD message is not sent to the client.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to enable the gateway (instead of the client) to send DPD messages to the client. Internet Key Exchange (IKE) DPD is a new keepalive scheme that sends messages to let the router know that the client is still connected.

Examples

The following example shows that DPD messages have been configured to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp profile vpnprofile
  keepalive 60 retry 5
```

kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** command in global configuration mode. To make Kerberos optional, use the **no** form of this command.

kerberos clients mandatory

no kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If this command is not configured and the user has Kerberos credentials stored locally, the **rsh**, **rcp**, **rlogin**, and **telnet** commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for **rcp** and **rsh** are used to negotiate.

Examples

The following example causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** command in global configuration mode. To turn off forwarding of Kerberos credentials, use the **no** form of this command.

kerberos credentials forward

no kerberos credentials forward

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Enable credentials forwarding to have users' ticket granting tickets (TGTs) forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

Examples

The following example forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** command in global configuration mode. To remove a Kerberos instance map, use the **no** form of this command.

kerberos instance map *instance privilege-level*

no kerberos instance map *instance*

Syntax Description	
<i>instance</i>	Name of a Kerberos instance.
<i>privilege-level</i>	The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.

Defaults Privilege level 1

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Use this command to create user instances with access to administrative commands.

Examples The following example sets the privilege level to 15 for authenticated Kerberos users with the *admin* instance in Kerberos realm:

```
kerberos instance map admin 15
```

Related Commands	Command	Description
	aaa authorization	Sets parameters that restrict user access to a network.

kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** command in global configuration mode. To remove the specified Kerberos realm from this router, use the **no** form of this command.

kerberos local-realm *kerberos-realm*

no kerberos local-realm

Syntax Description

<i>kerberos-realm</i>	The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters.
-----------------------	---

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

Examples

The following example specify the Kerberos realm in which the router is located as EXAMPLE.COM:

```
kerberos local-realm EXAMPLE.COM
```

Related Commands

Command	Description
kerberos preauth	Specifies a preauthentication method to use to communicate with the KDC.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos preauth

To specify a preauthentication method to use to communicate with the key distribution center (KDC), use the **kerberos preauth** command in global configuration mode. To disable Kerberos preauthentication, use the **no** form of this command.

kerberos preauth [**encrypted-unix-timestamp** | **encrypted-kerberos-timestamp** | **none**]

no kerberos preauth

Syntax Description	
encrypted-unix-timestamp	(Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.
encrypted-kerberos-timestamp	(Optional) Use the RFC1510 kerberos timestamp as a quick authentication method when communicating with the KDC.
none	(Optional) Do not use Kerberos preauthentication.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of **kerberos preauth**. If that happens, turn off the preauthentication with the **none** option.

The **no** form of this command is equivalent to using the **none** keyword.

Examples The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

Related Commands	Command	Description
	kerberos local-realm	Specifies the Kerberos realm in which the router is located.
	kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos realm

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the **kerberos realm** command in global configuration mode. To remove a Kerberos realm map, use the **no** form of this command.

```
kerberos realm {dns-domain | host} kerberos-realm
```

```
no kerberos realm {dns-domain | host} kerberos-realm
```

Syntax Description

<i>dns-domain</i>	Name of a DNS domain or host.
<i>host</i>	Name of a DNS host.
<i>kerberos-realm</i>	Name of the Kerberos realm to which the specified domain or host belongs.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

Examples

The following example maps the domain name “example.com” to the Kerberos realm, EXAMPLE.COM:

```
kerberos realm .example.com EXAMPLE.COM
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server** command in global configuration mode. To remove a Kerberos server for a specified Kerberos realm, use the **no** form of this command.

```
kerberos server kerberos-realm {host-name | ip-address} [port-number]
```

```
no kerberos server kerberos-realm {host-name | ip-address}
```

Syntax Description

<i>kerberos-realm</i>	Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
<i>host-name</i>	Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).
<i>ip-address</i>	IP address of the host functioning as the Kerberos server for the specified Kerberos realm.
<i>port-number</i>	(Optional) Port that the key distribution center (KDC) monitors (defaults to 88).

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use the **kerberos server** command to specify the location of the Kerberos server for a given realm.

Examples

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm EXAMPLE.COM:

```
kerberos server EXAMPLE.COM 192.168.47.66
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab entry** command in global configuration mode. To remove a SRVTAB entry from the router's configuration, use the **no** form of this command.

kerberos srvtab entry *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*

no kerberos srvtab entry *kerberos-principal principal-type*

Syntax Description

<i>kerberos-principal</i>	A service on the router.
<i>principal-type</i>	Version of the Kerberos SRVTAB.
<i>timestamp</i>	Number representing the date and time the SRVTAB entry was created.
<i>key-version number</i>	Version of the encryption key format.
<i>key-type</i>	Type of encryption used.
<i>key-length</i>	Length, in bytes, of the encryption key.
<i>encrypted-keytab</i>	Secret key the router shares with the key distribution center (KDC). It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** router configuration command to write the router's running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on to a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.

If you change the private DES key and reload an old version of the router's configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on to the router using the **kerberos srvtab remote** command.

Although you can configure **kerberos srvtab entry** on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the **kerberos srvtab remote** command.

Examples

In the following example, host/new-router.example.com@EXAMPLE.COM is the host, 0 is the type, 817680774 is the timestamp, 1 is the version of the key, 1 indicates the DES is the encryption type, 8 is the number of bytes, and .cCN.YoU.okK is the encrypted key:

```
kerberos srvtab entry host/new-router.example.com@EXAMPLE.COM 0 817680774 1 1 8
.cCN.YoU.okK
```

Related Commands

Command	Description
kerberos srvtab remote	Retrieves a krb5 SRVTAB file from the specified host.
key config-key	Defines a private DES key for the router.

kerberos srvtab remote

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the **kerberos srvtab remote** command in global configuration mode.

```
kerberos srvtab remote {boot_device:URL}
```

Syntax Description	URL	Machine that has the Kerberos SRVTAB file.
	<i>ip-address</i>	IP address of the machine that has the Kerberos SRVTAB file.
	<i>filename</i>	Name of the SRVTAB file.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines When you use the **kerberos srvtab remote** command to copy the SRVTAB file from the remote host (generally the key distribution center [KDC]), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write the router's running configuration to NVRAM.

Examples The following example copies the SRVTAB file residing on b1.example.com to a router named s1.example.com:

```
kerberos srvtab remote tftp://b1.example.com/s1.example.com-new-srvtab
```

Related Commands	Command	Description
	kerberos srvtab entry	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.
	key config-key	Defines a private DES key for the router.

key (isakmp-group)

To specify the Internet Key Exchange (IKE) preshared key for group policy attribute definition, use the **key** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a preshared key, use the **no** form of this command.

key *name*

no key *name*

Syntax Description

<i>name</i>	IKE preshared key that matches the password entered on the client.
Note	This value must match the “password” field that is defined in the Cisco VPN Client 3.x configuration GUI.

Defaults

No default behavior or values.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **key** command to specify the IKE preshared key when defining group policy information for Mode Configuration push. (It follows the **crypto isakmp client configuration group** command.) You *must* configure this command if the client identifies itself to the router with a preshared key. (You do not have to enable this command if the client uses a certificate for identification.)

Examples

The following example shows how to specify the preshared key “cisco”:

```
crypto isakmp client configuration group default
  key cisco
  dns 2.2.2.2 2.3.2.3
  pool dog
  acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

key config-key

To define a private DES key for the router, use the **key config-key** command in global configuration mode. To delete a private Data Encryption Standard (DES) key from the router, use the **no** form of this command.

key config-key 1 *string*

no key config-key 1 *string*

Syntax Description

1	Key number. This number is always 1.
<i>string</i>	Private DES key (can be up to eight alphanumeric characters).

Defaults

No DES-key defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was released.

Usage Guidelines

This command defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router's configuration.



Caution

The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

Examples

The following example sets *keyxx* as the private DES key on the router:

```
key config-key 1 keyxx
```

Related Commands

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

key config-key password-encryption

To store a type 6 encryption key in private NVRAM, use the **key config-key password-encryption** command in global configuration mode. To disable the encryption, use the **no** form of this command.

key config-key password-encryption [*text*]

no key config-key password-encryption [*text*]

Syntax Description

text (Optional) Password or master key.

Note It is recommended that you do not use the *text* argument but instead use interactive mode (using the enter key after you enter the **key config-key password-encryption** command) so that the preshared key will not be printed anywhere and, therefore, cannot be seen.

Defaults

No type 6 password encryption

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command, the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.



Caution

If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can “read” the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot “know” what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encryption key is to be stored in NVRAM:

```
Router (config)# key config-key password-encryption
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
password logging	Provides a log of debugging output for a type 6 password operation.

keyring

To configure a keyring with an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **keyring** command in ISAKMP profile configuration mode. To remove the keyring from the ISAKMP profile, use the **no** form of this command.

keyring *keyring-name*

no keyring *keyring-name*

Syntax Description

<i>keyring-name</i>	The keyring name, which must match the keyring name that was defined in the global configuration.
---------------------	---

Defaults

If this command is not used, the ISAKMP profile uses the keys defined in the global configuration.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile. If no keyring is defined in the profile, the global keys that were defined in the global configuration are used.

Examples

The following example shows that “vpnkeyring” is configured as the keyring name:

```
crypto isakmp profile vpnprofile
  keyring vpnkeyring
```

key-string (IKE)

To specify the Rivest, Shamir, and Adelman (RSA) public key of the remote peer, use the **key-string** command in public key configuration mode. To remove the RSA public key, use the **no** form of this command.

key-string *key-string*

no key-string *key-string*

Syntax Description

<i>key-string</i>	Enter the key in hexadecimal format. While entering the key data, you can press Return to continue entering data.
-------------------	---

Defaults

No default behavior or values

Command Modes

Public key configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Before using this command, you must enter the **rsa-pubkey** command in the crypto keyring mode. If possible, to avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

To complete the command, you must return to the global configuration mode by typing **quit** at the config-pubkey prompt.

Examples

The following example manually specifies the RSA public keys of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands	Command	Description
	crypto keyring	Defines a crypto keyring.
	rsa-pubkey	Defines the RSA public key to be used for encryption or signatures during IKE authentication.
	show crypto keyring	Displays keyrings on your router.

lifetime (certificate server)

To specify the lifetime of the certification authority (CA) or a certificate, use the **lifetime** command in certificate server configuration mode. To return to the default lifetime values, use the **no** form of this command.

lifetime { **ca-certificate** | **certificate** } *time*

no lifetime { **ca-certificate** | **certificate** } *time*

Syntax Description

ca-certificate	Lifetime is for the CA certificate of the certificate server.
certificate	Lifetime is for the certificate of the certificate server. The maximum certificate lifetime is one month less than the expiration date of the CA certificate's lifetime.
<i>time</i>	Lifetime value in days. Valid values range from 1 day to 1825 days. All certificates are valid on the date that they are issued.

Defaults

The default CA certificate lifetime is 3 years.

The default certificate lifetime is 1 year.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

After you enable a certificate server via the **crypto pki server** command, use the **lifetime** command if you wish to specify lifetime values other than the default values for the CA certificate and the certificate of the certificate server.

After the certificate generates its signed certificate, the lifetime cannot be changed.

Examples

The following example shows how to set the lifetime value for the CA to 30 days:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime ca certificate 30
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.

lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the **lifetime** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description	<i>seconds</i>	Number of many seconds for each each SA should exist before expiring. Use an integer from 60 to 86,400 seconds, which is the default value.
---------------------------	----------------	---

Defaults	86,400 seconds (one day)
-----------------	--------------------------

Command Modes	ISAKMP policy configuration
----------------------	-----------------------------

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines	Use this command to specify how long an IKE SA exists before expiring.
-------------------------	--

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPsec SAs. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPsec SAs. New IPsec SAs are negotiated before current IPsec SAs expire.

So, to save setup time for IPsec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note that when your local peer initiates an IKE negotiation between itself and a remote peer, an IKE policy can be selected only if the lifetime of the remote peer's policy is shorter than or equal to the lifetime of the local peer's policy. Then, if the lifetimes are not equal, the shorter lifetime will be selected. To restate this behavior: If the two peer's policies' lifetimes are not the same, the initiating peer's lifetime must be longer and the responding peer's lifetime must be shorter, and the shorter lifetime will be used.

Examples	The following example configures an IKE policy with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:
-----------------	--

```
crypto isakmp policy 15
  lifetime 600
exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
show crypto isakmp policy	Displays the parameters for each IKE policy.

lifetime crl

To define the lifetime of the certificate revocation list (CRL) that is used by the certificate server, use the **lifetime crl** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime crl *time*

no lifetime crl *time*

Syntax Description	<i>time</i>	Lifetime value, in hours, of the CRL. Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).
---------------------------	-------------	---

Defaults	168 hours (1 week)
-----------------	--------------------

Command Modes	Certificate server configuration
----------------------	----------------------------------

Command History	Release	Modification
	12.3(4)T	This command was introduced.

Usage Guidelines

After you create a certificate server via the **crypto pki server** command, use the **lifetime crl** command if you want to specify a value other than the default value for the CRL. The lifetime value is added to the CRL when the CRL is created.

The CRL is written to the specified database location as *ca-label.crl*.

Examples

The following example shows how to set the lifetime value for the CRL to 24 hours:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime crl 24
```

Related Commands	Command	Description
	cdp-url	Specifies that CDP should be used in the certificates that are issued by the certificate server.
	crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

lifetime enrollment-request

To specify how long an enrollment request should stay in the enrollment database, use the **lifetime enrollment-request** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime enrollment-request *time*

no lifetime enrollment-request

Syntax Description

<i>time</i>	Lifetime value, in hours, of an enrollment request. The maximum lifetime value is 1000 hours. The default value is 168 hours (1 week).
-------------	--

Defaults

Lifetime value default is 168 hours.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. The request is left in the Enrollment Request Database for the lifetime of the enrollment request until the client polls the certificate server for the result of the request.

Examples

The following example shows how to set the lifetime value for the enrollment request to 24 hours:

```
Router (config)# crypto pki server mycs
Router (cs-server)# lifetime enrollment-request 24
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki server grant	Grants all or certain SCEP requests.
crypto pki server remove	Removes enrollment requests that are in the certificate server Enrollment Request Database.

li-view

To initialize a lawful intercept view, use the **li-view** command in global configuration mode.

li-view *li-password* **user** *username* **password** *password*

Syntax Description

<i>li-password</i>	Associates the lawful interface view with a password. The password can contain any number of alphanumeric characters. Note The password is case sensitive.
user <i>username</i>	User who can access the lawful intercept view.
password <i>password</i>	Associates a password with the specified user <i>username</i> option; that is, the user must provide the specified password to access the view.

Defaults

A lawful intercept view cannot be accessed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Like a command-line interface (CLI) view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that stores information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level.
- CLI that are useful for lawful intercept users but do not need to be excluded from other views or privilege levels.



Note

Only a system administrator or a level 15 privilege user can initialize a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added to the view:

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# end
```

```
! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
```

```

Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of 'running-configuration'.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#

```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.
username	Establishes a username-based authentication system.

local-address

To limit the scope of an Internet Security Association and Key Management Protocol (ISAKMP) profile or an ISAKMP keyring configuration to a local termination address or interface, use the **local-address** command in ISAKMP profile configuration and keyring configuration modes. To remove the local address or interface, use the **no** form of this command.

local-address {*interface-name* | *ip-address* [*vrf-tag*]}

no local-address {*interface-name* | *ip-address* [*vrf-tag*]}

Syntax Description		
	<i>interface-name</i>	Name of the local interface.
	<i>ip-address</i>	Local termination address.
	<i>vrf-tag</i>	(Optional) Scope of the IP address will be limited to the VRF instance.

Defaults If this command is not configured, the ISAKMP profile or ISAKMP keyring is available to all local addresses.

Command Modes ISAKMP profile configuration
Keyring configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.
	12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Examples The following example shows that the scope of the ISAKMP profile is limited to interface serial2/0:

```
crypto isakmp profile profile1
  keyring keyring1
  match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

The following example shows that the scope of the ISAKMP keyring is limited only to interface serial2/0:

```
crypto keyring
  local-address serial2/0
  pre-shared-key address 10.0.0.1
```

The following example shows that the scope of the ISAKMP keyring is limited only to IP address 10.0.0.2:

```
crypto keyring keyring1
  local-address 10.0.0.2
  pre-shared-key address 10.0.0.2 key
```

The following example shows that the scope of an ISAKMP keyring is limited to IP address 10.34.35.36 and that the scope is limited to VRF examplevrf1:

```
ip vrf examplevrf1
  rd 12:3456
crypto keyring ring1
  local-address 10.34.35.36 examplevrf1
interface ethernet2/0
  ip vrf forwarding examplevrf1
  ip address 10.34.35.36 255.255.0.0
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPsec user sessions.
crypto keyring	Defines a keyring and enters keyring configuration mode.

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication** command in line configuration mode. To return to the default specified by the **aaa authentication login** command, use the **no** form of this command.

login authentication { **default** | *list-name* }

no login authentication { **default** | *list-name* }

Syntax Description

default	Uses the default list created with the aaa authentication login command.
<i>list-name</i>	Uses the indicated list created with the aaa authentication login command.

Defaults

Uses the default set with **aaa authentication login**.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).



Caution

If you use a *list-name* value that was not configured with the **aaa authentication login** command, you will disable login on this line.

Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login** command.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
 login authentication default
```

The following example specifies that the AAA authentication list called *list1* is to be used on line 7:

```
line 7
 login authentication list1
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

login block-for

To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the **login block-for** command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the **no** form of this command.

login block-for *seconds* **attempts** *tries* **within** *seconds*

no login block-for

Syntax Description

<i>seconds</i>	Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.
attempts <i>tries</i>	Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.
within <i>seconds</i>	Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.

Defaults

No login parameters are defined.
A quiet period is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25).

Usage Guidelines

If the specified number of connection attempts (via the **attempts** *tries* option) fail within a specified time (via the **within** *seconds* option), the Cisco IOS device will not accept any additional login attempts for a specified period of time (via the *seconds* argument).

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of 1 second
- All login attempts made via Telnet, secure shell (SSH), and HTTP are denied during the quiet period; that is, no access control lists (ACLs) are exempt from the login period until the **login quiet-mode access-class** command is issued.

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the **show login** command is issued to verify the login settings.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# exit
Router# show login
```

```
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
```

```
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
```

```
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5
```

The following example shows how to disable login parameters. Thereafter, the **show login** command is issued to verify that login parameters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
Router# show login
```

```
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
```

```
Router NOT enabled to watch for login Attacks
```

Related Commands

Command	Description
login delay	Configures a uniform delay between successive login attempts.
login on-failure	Generates system logging messages for failed login attempts.
login on-success	Generates system logging messages for successful login attempts.
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.
show login	Displays login parameters.

login delay

To configure a uniform delay between successive login attempts, use the **login delay** command in global configuration mode. To return to the default functionality (which is a 1 second delay), use the **no** form of this command.

login delay *seconds*

no login delay

Syntax Description

<i>seconds</i>	Number of seconds between each login attempt. Valid values range from 1 to 10 seconds.
----------------	--

Defaults

If this command is not enabled, a login delay of 1 second is automatically enforced.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

A Cisco IOS device can accept connections (such as Telnet, secure shell (SSH), and HTTP) as fast as they can be processed. The **login delay** command introduces a uniform delay between successive login attempts. (The delay occurs for all login attempts—failed or successful attempts.) Thus, user users can better secure their Cisco IOS device from dictionary attacks, which are an attempt to gain username and password access to your device.

Although the **login delay** command allows users to configure a specific a delay, a uniform delay of 1 second is enabled if the **auto secure** command is issued. After the **auto secure** command is enabled, the autosecure dialog prompts users for login parameters; if login parameters have already been configured, the autosecure dialog will retain the specified values.

Examples

The following example shows how to configure your router to issue a delay of 10 seconds between each successive login attempt:

```
Router(config)# login delay 10
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login on-failure

To generate logging messages for failed login attempts, use the **login on-failure** command in global configuration mode. To disable logging messages, use the **no** form of this command.

login on-failure log [*every login*]

no login on-failure log [*every login*]

Syntax Description

log	Logging messages are generated.
every login	(Optional) Number of failed login attempts that must occur before a logging message is generated; that is, a logging message is not generated for every failed login attempt. The default value is one attempt. Valid values range from 1 to 65535 attempts.

Defaults

Logging messages are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Logging messages allow users to receive notice for every failed login attempt that is made to their device. This functionality is automatically enabled when the **auto secure** command is issued.



Note

Currently, only logging messages can be generated for login-related events. Support for simple network management protocol (SNMP) traps will be added in a later release.

Examples

The following example shows how to enable logging messages for every fifth failed login attempt:

```
Router(config)# login on-failure log every 5
```

The following logging message is generated upon a failed login request:

```
00:03:34:%SEC_LOGIN-4-LOGIN_FAILED:Login failed [user:sdfs] [Source:10.4.2.11]
[localport:23] [Reason:Invalid login] at 20:54:42 UTC Fri Feb 28 2003
```

Related Commands	Command	Description
	auto secure	Secures the management and forwarding planes of the router.
	login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
	login on-success	Generates system logging messages for successful login attempts.
	show login	Displays login parameters.

login on-success

To generate logging messages for successful login attempts, use the **login on-success** command in global configuration mode. To disable logging messages, use the **no** form of this command.

login on-success log [*every login*]

no login on-success log [*every login*]

Syntax Description

log	Logging messages are generated.
every login	(Optional) Number of failed login attempts that must occur before a logging message is generated; that is, a logging message is not generated for every failed login attempt. The default value is one attempt. Valid values range from 1 to 65535 attempts.

Defaults

Logging messages are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Logging messages allow users to receive notice for every successful login that is made to their device.



Note

Currently, only logging messages can be generated for login-related events. Support for simple network management protocol (SNMP) traps will be added in a later release.

Examples

The following example shows how to enable logging messages for every fifth successful login attempt:

```
Router(config)# login on-success log every 5
```

The following logging message is generated upon a successful login request:

```
00:04:32:%SEC_LOGIN-5-LOGIN_SUCCESS:Login Success [user:test] [Source:10.4.2.11]
[localport:23] at 20:55:40 UTC Fri Feb 28 2003
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.

Command	Description
login on-failure	Generates system logging messages for failed login attempts.
show login	Displays login parameters.

login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the **login quiet-mode access-class** command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the **no** form of this command.

```
login quiet-mode access-class {acl-name | acl-number}
```

```
no login quiet-mode access-class {acl-name | acl-number}
```

Syntax Description

<i>acl-name</i>	Named ACL that is to be enforced during quiet mode.
<i>acl-number</i>	Numbered (standard or extended) ACL that is to be enforced during quiet mode.

Defaults

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Before using this command, you must issue the **login block-for** command, which allows you to specify the necessary parameters to enable a quiet period.

Use the **login quiet-mode access-class** command to selectively allow hosts on the basis of a specified ACL. You may use this command to grant an active client or list of clients an infinite number of failed attempts that are not counted by the router; that is, the active clients are placed on a “safe list” that allows them access to the router despite a quiet period.

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to accept hosts only from the ACL “myacl” during the next quiet period:

```
Router(config)# login quiet-mode access-class myacl
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login-message

To configure a message for a user login text box on the login page, use the **login-message** command in Web VPN configuration mode. To reset the value to the default, use the **no** form of this command.

login-message *message-string*

no login-message *message-string*

Syntax Description

<i>message-string</i>	Limited to 255 characters. The default is “Please enter your username and password.” The string value may contain 7-bit ASCII values, HTML tags, and escape sequences. To have no login message, the login-message command is issued without a string.
-----------------------	---

Defaults

Message will be “Please enter your username and password.”

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

If you type the **login-message** command and then press the **Enter** key, no login message will be displayed.

Examples

The following example shows that the login message to be displayed is “Please enter your login credentials.”

```
Router (config-webvpn)# login-message "Please enter your login credentials."
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

logo

To specify the custom logo image that is displayed on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **logo** command in Web VPN configuration mode. To remove the logo, use the **no** form of this command.

logo [**file** *filename* | **none**]

no logo [**file** *filename* | **none**]

Syntax Description

file <i>filename</i>	<i>(Optional) Limited to 255 characters. The logo must be a GIF, JPG, or PNG file and must be less than 100 kilobytes (KBs). An error will occur if the file does not exist. If the logo file is subsequently deleted, no logo is displayed. The default is to use the Cisco logo.</i>
none	<i>(Optional) No logo will be displayed.</i>

Defaults

No logo is displayed.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows that a logo file (mylogo.gif) is being configured in flash: media:

```
logo file flash:/mylogo.gif
```

The following example shows that no logo is to be displayed in the login or portal pages:

```
logo none
```

The following example shows that the logo is set to the default logo, which is the Cisco logo:

```
no logo
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

mac-address (RITE)

To specify the Ethernet address of the destination host, use the **mac-address** command in router IP traffic export (RITE) configuration mode. To change the MAC address of the destination host, use the **no** form of this command.

mac-address *H.H.H*

no mac-address *H.H.H*

Syntax Description	<i>H.H.H</i>	48-bit MAC address.
--------------------	--------------	---------------------

Defaults A destination host is not known.

Command Modes RITE configuration

Command History	Release	Modification
	12.3(4)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines The **mac-address** command, which is used to specify the destination host that is receiving the exported traffic, is part of suite of RITE configuration mode commands that are used to control various attributes for both incoming and outgoing IP traffic export.

The **ip traffic-export profile** command allows you to begin a profile that can be configured to export IP packets as they arrive or leave a selected router ingress interface. A designated egress interface exports the captured IP packets out of the router. Thus, the router can export unaltered IP packets to a directly connected device.

Examples The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control lists (ACL) “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.

match address (IPSec)

To specify an extended access list for a crypto map entry, use the **match address** command in crypto map configuration mode. To remove the extended access list from a crypto map entry, use the **no** form of this command.

match address [*access-list-id* | *name*]

no match address [*access-list-id* | *name*]

Syntax Description

<i>access-list-id</i>	(Optional) Identifies the extended access list by its name or number. This value should match the <i>access-list-number</i> or <i>name</i> argument of the extended access list being matched.
<i>name</i>	(Optional) Identifies the named encryption access list. This name should match the <i>name</i> argument of the named encryption access list being matched.

Defaults

No access lists are matched to the crypto map entry.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command is required for all static crypto map entries. If you are defining a dynamic crypto map entry (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use this command to assign an extended access list to a crypto map entry. You also need to define this access list using the **access-list** or **ip access-list extended** commands.

The extended access list specified with this command will be used by IPSec to determine which traffic should be protected by crypto and which traffic does not need crypto protection. (Traffic that is permitted by the access list will be protected. Traffic that is denied by the access list will not be protected in the context of the corresponding crypto map entry.)

Note that the crypto access list is *not* used to determine whether to permit or deny traffic through the interface. An access list applied directly to the interface makes that determination.

The crypto access list specified by this command is used when evaluating both inbound and outbound traffic. Outbound traffic is evaluated against the crypto access lists specified by the interface's crypto map entries to determine if it should be protected by crypto and if so (if traffic matches a **permit** entry) which crypto policy applies. (If necessary, in the case of static IPSec crypto maps, new security associations are established using the data flow identity as specified in the **permit** entry; in the case of dynamic crypto map entries, if no SA exists, the packet is dropped.) After passing the regular access lists at the interface, inbound traffic is evaluated against the crypto access lists specified by the entries of the

interface's crypto map set to determine if it should be protected by crypto and, if so, which crypto policy applies. (In the case of IPSec, unprotected traffic is discarded because it should have been protected by IPSec.)

In the case of IPSec, the access list is also used to identify the flow for which the IPSec security associations are established. In the outbound case, the **permit** entry is used as the data flow identity (in general), while in the inbound case the data flow identity specified by the peer must be "permitted" by the crypto access list.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the security associations. (This example is for a static crypto map.)

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association level per-host	Specifies that separate IPSec security associations should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

match certificate (ca-trustpoint)

To associate a certificate-based access control list (ACL) that is defined with the **crypto ca certificate map** command, use the **match certificate** command in ca-trustpoint configuration mode. To remove the association, use the **no** form of this command.

match certificate *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**]

no match certificate *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**]

Syntax Description

<i>certificate-map-label</i>	Matches the <i>label</i> argument specified in a previously defined crypto ca certificate map command.
allow expired-certificate	(Optional) Ignores expired certificates. Note If this keyword is not configured, the router does not ignore expired certificates.
skip revocation-check	(Optional) Allows a trustpoint to enforce certificate revocation lists (CRLs) except for specific certificates. Note If this keyword is not configured, the trustpoint enforces CRLs for all certificates.
skip authorization-check	(Optional) Skips the authentication, authorization, and accounting (AAA) check of a certificate when public key infrastructure (PKI) integration with an AAA server is configured. Note If this keyword is not configured and PKI integration with an AAA server is configured, the AAA checking of a certificate is done.

Defaults

If this command is not configured, no default match certificate is configured. Each of the **allow expired-certificate**, **skip revocation-check**, and **skip authorization-check** keywords have a default (see the “Syntax Description” section).

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(4)T	The allow expired-certificate , skip revocation-check , and skip authorization-check keywords were added.

Usage Guidelines

The **match certificate** command associates the certificate-based ACL defined with the **crypto ca certificate map** command to the trustpoint. The *certificate-map-label* argument in the **match certificate** command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

The certificate map with the label *certificate-map-label* must be defined before it can be used with the **match certificate** subcommand.

A certificate referenced in a **match certificate** command may not be deleted until all references to the certificate map are removed from configured trustpoints (that is, no **match certificate** commands can reference the certificate map being deleted).

When the certificate of a peer has been verified, the certificate-based ACL as specified by the certificate map is checked. If the certificate of the peer matches the certificate ACL, or a certificate map is not associated with the trustpoint used to verify the certificate of the peer, the certificate of the peer is considered valid.

If the certificate map does not have any attributes defined, the certificate is rejected.

Using the **allow expired-certificate** Keyword

The **allow expired-certificate** keyword has two purposes:

- If the certificate of a peer has expired, this keyword may be used to “allow” the expired certificate until the peer is able to obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This keyword may be used to allow the certificate of the peer even though your router clock is not set.



Note

- If Network Time Protocol (NTP) is available only via the IPSec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be “brought up” because the certificate of the hub is not yet valid.
- “Expired” is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end time specified in the certificate.

Using the **skip revocation-check** Keyword

The type of enforcement provided using the **skip revocation-check** keyword is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. If one spoke communicates directly with another spoke, the CRLs must be checked. However, if the trustpoint is configured to require CRLs, the connection to the hub to retrieve the CRL usually cannot be made because the CRL is available only via the connection hub.

Using the **skip authorization-check** Keyword

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the **skip authorization-check** keyword. For example, if a Virtual Private Network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the **skip authorization-check** keyword to skip the certificate check so that the tunnel can be established.

The **skip authorization-check** keyword should be configured after PKI integration with an AAA server is configured.

Examples

The following example shows a certificate-based ACL with the label “Group” defined in a **crypto ca certificate map** command and included in the **match certificate** command:

```
crypto ca certificate map Group 10
  subject-name co ou=WAN
  subject-name co o=Cisco
!
crypto ca trustpoint pki
  match certificate Group
```

The following example shows a configuration for a central site using the **allow expired-certificate** keyword. The router at a branch site has an expired certificate named “branch1” and has to establish a tunnel to the central site to renew its certificate.

```
crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Central VPN Gateway
  revocation-check crl
  match certificate branch1 allow expired-certificate
```

The following example shows a branch office configuration using the **skip revocation-check** keyword. The trustpoint is being allowed to enforce CRLs except for “central-site” certificates.

```
crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
  match certificate central-site skip revocation-check
```

The following example shows a branch office configuration using the **skip authorization-check** keyword. The trustpoint is being allowed to skip AAA checking for the central site.

```
crypto pki trustpoint home-office
  auth list allow_list
  auth user subj commonname
  match certificate central-site skip authorization-check
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match certificate (ISAKMP)

To assign an Internet Security Association Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate, use the **match certificate** command in crypto ISAKMP profile configuration mode. To remove the profile, use the **no** form of this command.

match certificate *certificate-map*

no match certificate *certificate-map*

Syntax Description

<i>certificate-map</i>	Name of the certificate map.
------------------------	------------------------------

Defaults

No default behavior or values

Command Modes

Crypto ISAKMP profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **match certificate** command is used after the certificate map has been configured and the ISAKMP profiles have been assigned to them.

Examples

The following configuration example shows that whenever a certificate contains “ou = green,” the ISAKMP profile “cert_pro” will be assigned to the peer.

```
crypto pki certificate map cert_map 10
  subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
  ca trust-point 2315
  ca trust-point LaBCA
  initiate mode aggressive
  match certificate cert_map
```

Related Commands

Command	Description
client configuration group	Associates a group with the peer that has been assigned an ISAKMP profile.

match certificate override cdp

To manually override the existing certificate distribution point (CDP) entries for a certificate with a URL or directory specification, use the **match certificate override cdp** command in ca-trustpoint configuration mode. To remove the override, use the **no** form of this command.

```
match certificate certificate-map-label override cdp {url | directory} string
```

```
no match certificate certificate-map-label override cdp {url | directory} string
```

Syntax Description

<i>certificate-map-label</i>	A user-specified label that must match the <i>label</i> argument specified in a previously defined crypto ca certificate map command.
url	Specifies that the certificates CDPs will be overridden with an http or ldap URL.
directory	Specifies that the certificate's CDPs will be overridden with an ldap directory specification.
<i>string</i>	The URL or directory specification.

Defaults

The existing CDP entries for the certificate are used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Usage Guidelines

Use the **match certificate override cdp** command to replace all of the existing CDPs in a certificate with a manually configured CDP URL or directory specification.

The *certificate-map-label* argument in the **match certificate override cdp** command must match the *label* argument specified in a previously defined **crypto ca certificate map** command.



Note

Some applications may time out before all CDPs have been tried and will report an error message. This will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.

Examples

The following example uses the **match certificate override cdp** command to override the CDPs for the certificate map named Group1 defined in a **crypto ca certificate map** command:

```
crypto ca certificate map Group1 10
  subject-name co ou=WAN
  subject-name co o=Cisco
!
```

■ **match certificate override cdp**

```
crypto ca trustpoint pki
  match certificate Group1 override cdp url http://server.cisco.com
```

Related Commands

Command	Description
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

match identity

To match an identity from a peer in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **match identity** command in ISAKMP profile configuration mode. To remove the identity, use the **no** form of this command.

```
match identity { group group-name | address address [mask] [fvr] | host host-name | host domain domain-name | user user-fqdn | user domain domain-name }
```

```
no match identity { group group-name | address address [mask] [fvr] | host host-name | host domain domain-name | user user-fqdn | user domain domain-name }
```

Syntax Description

group <i>group-name</i>	A Unity group that matches identification (ID) type ID_KEY_ID. If Unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the <i>group-name</i> argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
address <i>address</i> [<i>mask</i>] [<i>fvr</i>]	An identity that matches the identity of type ID_IPV4_ADDR. <ul style="list-style-type: none"> <i>mask</i>—Use to match the range of the address. <i>fvr</i>—Use to match the address in the front door Virtual Route Forwarding (FVRF) Virtual Private Network (VPN) space.
host <i>host-name</i>	Identity that matches an identity of the type ID_FQDN.
host domain <i>domain-name</i>	Identity that matches an identity of the type ID_FQDN, whose fully qualified domain name (FQDN) ends with the domain name.
user <i>user-fqdn</i>	Identity that matches the FQDN.
user domain <i>domain-name</i>	Identity that matches the identities of the type ID_USER_FQDN. When the user domain keyword is present, all users having identities of the type ID_USER_FQDN and ending with “ <i>domain-name</i> ” will be matched.

Defaults

No default behavior or values

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

There must be at least one **match identity** command in an ISAKMP profile configuration. The peers are mapped to an ISAKMP profile when their identities are matched (as given in the ID payload of the Internet Key Exchange [IKE] exchange) against the identities that are defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid.

Examples

The following example shows that the **match identity** command is configured:

```
crypto isakmp profile vpnprofile
  match identity group vpngroup
  match identity address 10.53.11.1
  match identity host domain vpn.com
  match identity host server.vpn.com
```

max-header-length

To permit or deny HTTP traffic on the basis of the message header length, use the **max-header-length** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

max-header-length { **request** *bytes* **response** *bytes* } **action** { **reset** | **allow** } [**alarm**]

no max-header-length { **request** *bytes* **response** *bytes* } **action** { **reset** | **allow** } [**alarm**]

Syntax Description

request <i>bytes</i>	Maximum header length, in bytes, allowed in the request message. Number of bytes range: 0 to 65535.
response <i>bytes</i>	Maximum header length, in bytes, allowed in the response message. Number of bytes range: 0 to 65535.
action	Messages that exceed the maximum size are subject to the specified action (reset or allow).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not issued, all traffic is permitted.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

All message header lengths exceeding the configured maximum size will be subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
  application http
    strict-http action allow alarm
    content-length maximum 1 action allow alarm
    content-type-verification match-req-rsp action allow alarm
    max-header-length request 1 response 1 action allow alarm
    max-uri-length 1 action allow alarm
    port-misuse default action allow alarm
```

```
request-method rfc default action allow alarm
request-method extension default action allow alarm
transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
ip inspect firewall in
!
!
```

max-logins

To limit the number of simultaneous logins for users in a specific server group, use the **max-logins** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-logins *number-of-users*

no max-logins *number-of-users*

Syntax Description

<i>number-of-users</i>	Number of logins. The value ranges from 1 through 10.
------------------------	---

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of simultaneous logins for users in that group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of logins for users in server group “cisco” has been set to 8:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-logins 8
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
max-users	Limits the number of connections to a specific server group.

max-uri-length

To permit or deny HTTP traffic on the basis of the uniform resource identifier (URI) length in the request message, use the **max-uri-length** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

max-uri-length *bytes* **action** { **reset** | **allow** } [**alarm**]

no max-uri-length *bytes* **action** { **reset** | **allow** } [**alarm**]

Syntax Description

<i>bytes</i>	Number of bytes ranging from 0 to 65535.
action	Messages that exceed the maximum URI length are subject to the specified action (reset or allow).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If this command is not issued, all traffic is permitted.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

All URI lengths exceeding the configured value will be subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
  application http
    strict-http action allow alarm
    content-length maximum 1 action allow alarm
    content-type-verification match-req-rsp action allow alarm
    max-header-length request 1 response 1 action allow alarm
    max-uri-length 1 action allow alarm
    port-misuse default action allow alarm
    request-method rfc default action allow alarm
    request-method extension default action allow alarm
    transfer-encoding type default action allow alarm
!
```

```
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

max-users

To limit the number of connections to a specific server group, use the **max-users** command in global configuration mode. To remove the number of connections that were set, use the **no** form of this command.

max-users *number-of-users*

no max-users *number-of-users*

Syntax Description	<i>number-of-users</i>	Number of users. The value ranges from 1 through 5000.
---------------------------	------------------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.

Usage Guidelines

The **crypto isakmp client configuration group** command must be configured before this command can be configured.

This command makes it possible to mimic the functionality provided by some RADIUS servers for limiting the number of connections to a specific server group.

The **max-users** and **max-logins** keywords can be enabled together or individually to control the usage of resources by any groups or individuals.

Examples

The following example shows that the maximum number of connections to server group “cisco” has been set to 1200:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config)# max-users 1200
```

The following shows the RADIUS attribute-value (AV) pairs for the maximum users and maximum logins parameters:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Related Commands	Command	Description
	crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
	max-logins	Limits the number of simultaneous logins for users in a specific server group.

mode (IPSec)

To change the mode for a transform set, use the **mode** command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the **no** form of this command.

mode [**tunnel** | **transport**]

no mode

Syntax Description	tunnel	(Optional) Specifies the mode for a transform set: either tunnel or transport mode.
	transport	If neither tunnel nor transport is specified, the default (tunnel mode) is assigned.

Defaults	Tunnel mode
-----------------	-------------

Command Modes	Crypto transform configuration
----------------------	--------------------------------

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines

Use this command to change the mode specified for the transform. This setting is only used when the traffic to be protected has the same IP addresses as the IPSec peers (this traffic can be encapsulated either in tunnel or transport mode). This setting is ignored for all other traffic (all other traffic is encapsulated in tunnel mode).

If the traffic to be protected has the same IP address as the IP Security peers and transport mode is specified, during negotiation the router will request transport mode but will accept either transport or tunnel mode. If tunnel mode is specified, the router will request tunnel mode and will accept only tunnel mode.

After you define a transform set, you are put into the crypto transform configuration mode. While in this mode you can change the mode to either tunnel or transport. This change applies only to the transform set just defined.

If you do not change the mode when you first define the transform set, but later decide you want to change the mode for the transform set, you must re-enter the transform set (specifying the transform name and all its transforms) and then change the mode.

If you use this command to change the mode, the change will only affect the negotiation of subsequent IPSec security associations via crypto map entries which specify this transform set. (If you want the new settings to take effect sooner, you can clear all or part of the security association database. See the **clear crypto sa** command for more details.

Tunnel Mode

With tunnel mode, the entire original IP packet is protected (encrypted, authenticated, or both) and is encapsulated by the IPSec headers and trailers (an Encapsulation Security Protocol header and trailer, an Authentication Header, or both). Then a new IP header is prefixed to the packet, specifying the IPSec endpoints as the source and destination.

Tunnel mode can be used with any IP traffic. Tunnel mode must be used if IPSec is protecting traffic from hosts behind the IPSec peers. For example, tunnel mode is used with Virtual Private Networks (VPNs) where hosts on one protected network send packets to hosts on a different protected network via a pair of IPSec peers. With VPNs, the IPSec peers “tunnel” the protected traffic between the peers while the hosts on their protected networks are the session endpoints.

Transport Mode

With transport mode, only the payload (data) of the original IP packet is protected (encrypted, authenticated, or both). The payload is encapsulated by the IPSec headers and trailers (an ESP header and trailer, an AH header, or both). The original IP headers remain intact and are not protected by IPSec.

Use transport mode only when the IP traffic to be protected has IPSec peers as both the source and destination. For example, you could use transport mode to protect router management traffic. Specifying transport mode allows the router to negotiate with the remote peer whether to use transport or tunnel mode.

Examples

The following example defines a transform set and changes the mode to transport mode. The mode value only applies to IP traffic with the source and destination addresses at the local and remote IPSec peers.

```
crypto ipsec transform-set newer esp-des esp-sha-hmac
mode transport
exit
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.

mode ra

To place the public key infrastructure (PKI) server into Registration Authority (RA) certificate server mode, use the **mode ra** command in certificate server configuration mode. To remove the PKI server from RA certificate mode, use the **no** form of this command.

mode ra

no mode ra

Syntax Description

This command has no arguments or keywords.

Defaults

The PKI server is not placed into RA certificate server mode.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS issuing certification authority (CA). If the **mode ra** command is not configured and the certificate server is enabled for the first time, a self-signed CA certificate will be generated and the certificate server will operate as a root CA.

Examples

The following configuration example shows that a RA mode certificate server named "myra" has been configured:

```
Router (config)# crypto pki trustpoint myra
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=cisco, c=us
Router (ca-trustpoint)# exit

Router (config)# crypto pki server myra
Router (cs-server)# mode ra
Router (cs-server)# no shutdown
```

Related Commands:

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki trustpoint	Declares the trustpoint that your router should use.
enrollment	Specifies the enrollment parameters of a CA.
show crypto pki server	Displays the current state and configuration of the certificate server.

mode sub-cs

To place the public key infrastructure (PKI) server into sub-certificate server mode, use the **mode sub-cs** command in certificate server mode. To remove the PKI server from sub-certificate mode, use the **no** form of this command.

mode sub-cs

no mode sub-cs

Syntax Description

This command has no arguments or keywords.

Defaults

The PKI server is not placed into sub-certificate server mode.

Command Modes

Certificate server

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS root certification authority (CA). If the **mode sub-cs** command is not configured and the certificate server is enabled for the first time, a self-signed CA certification will be generated and the certificate server will operate as a root CA.



Note

The **no mode sub-cs command** will have no effect if the server has been configured already. For example, if you want to make the subordinate CA a root CA, you must delete the server and re-create it.

Examples

The following configuration example shows that a subordinate certificate server named “sub” has been configured:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# exit

Router (config)# crypto pki server sub
Router (cs-server)# issuer-name CN=sub CA, O=Cisco, C=us
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki trustpoint	Declares the trustpoint that your router should use.

Command	Description
enrollment	Specifies the enrollment parameters of a CA.
issuer-name	Specifies the DN as the CA issuer name for the certificate server.
show crypto pki server	Displays the current state and configuration of the certificate server.

name (view)

To change the name of a lawful intercept view, use the **name** command in view configuration mode. To return to the default lawful intercept view name, which is “li-view,” use the **no** form of this command.

name *new-name*

no name *new-name*

Syntax Description

<i>new-name</i>	Lawful intercept view name.
-----------------	-----------------------------

Defaults

A lawful intercept view is called “li-view.”

Command Modes

View configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Only a system administrator or a level 15 privilege user can change the name of a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view and change the view name to “myliview”:

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# name myliview
Router(config-view)# end
```

Related Commands

Command	Description
li-view	Creates a lawful intercept view.
parser view	Creates or changes a CLI view and enters view configuration mode.

named-key

To specify which peer's RSA public key you will manually configure and enter public key configuration mode, use the **named-key** command in public key chain configuration mode. This command should be used only when the router has a single interface that processes IP Security (IPSec).

named-key *key-name* [**encryption** | **signature**]

Syntax Description		
	<i>key-name</i>	Specifies the name of the remote peer's RSA keys. This is always the fully qualified domain name of the remote peer; for example, router.example.com.
	encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special-usage key.
	signature	(Optional) Indicates that the RSA public key to be specified will be a signature special-usage key.

Defaults If neither the **encryption** nor the **signature** keyword is used, general-purpose keys will be specified.

Command Modes Public key chain configuration.

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines Use this command or the **addressed-key** command to specify which IPSec peer's RSA public key you will manually configure next.

Follow this command with the **key-string** command to specify the key.

If you use the **named-key** command, you also need to use the **address** public key configuration command to specify the IP address of the peer.

If the IPSec remote peer generated general purpose RSA keys, do not use the **encryption** or **signature** keyword.

If the IPSec remote peer generated special usage keys, you must manually specify both keys: perform this command and the **key-string** command twice and use the **encryption** and **signature** keywords in turn.

Examples The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-purpose keys.

```
crypto key pubkey-chain rsa
  named-key otherpeer.example.com
  address 10.5.5.1
  key-string
    005C300D 06092A86 4886F70D 01010105
    00034B00 30480241 00C5E23B 55D6AB22
```

```

04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
exit
addressed-key 10.1.1.2 encryption
key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
quit
exit
addressed-key 10.1.1.2 signature
key-string
0738BC7A 2BC3E9F0 679B00FE 098533AB
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
quit
exit
exit

```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
addressed-key	Specifies the RSA public key of the peer you will manually configure.
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

nas

To add an access point or router to the list of devices that use the local authentication server, use the **nas** command in local RADIUS server configuration mode. To remove the identity of the network access server (NAS) that is configured on the local RADIUS server, use the **no** form of this command

```
nas ip-address key shared-key
```

```
no nas ip-address key shared-key
```

Syntax Description

<i>ip-address</i>	IP address of the access point or router.
key	Specifies a key.
<i>shared-key</i>	Shared key that is used to authenticate communication between the local authentication server and the access points and routers that use this authenticator.

Defaults

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following command adds the access point having the IP address 192.168.12.17 to the list of devices that use the local authentication server, using the shared key “shared256.”

```
nas 192.168.12.17 key shared256
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.

Command	Description
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

no crypto engine software ipsec

To disable hardware crypto engine failover to the software crypto engine, use the **no crypto engine software ipsec** command in global configuration mode. To reenablen failover, use the **crypto engine software ipsec** form of this command.

no crypto engine software ipsec

crypto engine software ipsec

Syntax Description This command has no arguments or keywords.

Defaults Failover is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1E	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines Use this command for those situations in which the amount of IP Security (IPSec) traffic is more than can be handled (because of bandwidth) by the software routines on the CPU.

Examples The following example shows that hardware crypto engine failover to the software crypto engine has been disabled:

```
no crypto engine software ipsec
```

The following example shows that hardware crypto engine failover has been reenablen:

```
crypto engine software ipsec
```

Related Commands	Command	Description
	crypto engine accelerator	Enables the onboard hardware accelerator of the router for IPSec encryption.

no crypto xauth

To ignore extended authentication (Xauth) during an Internet Key Exchange (IKE) Phase 1 negotiation, use the **no crypto xauth** command in global configuration mode. To consider Xauth proposals, use the **crypto xauth** command.

no crypto xauth *interface*

crypto xauth *interface*

Syntax Description	<i>interface</i>	Interface whose IP address is the local endpoint to which the remote peer will send IKE requests.
---------------------------	------------------	---

Defaults	No default behaviors or values
-----------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines	The no version of this command was introduced to support Unity clients that do not require Xauth when using Internet Security Association and Key Management Protocol (ISAKMP) profiles.
-------------------------	---

Examples	The following example shows that Xauth proposals on Ethernet 1/1 are to be ignored: no crypto xauth Ethernet1/1
-----------------	--

no ip inspect

To turn off Context-based Access Control (CBAC) completely at a firewall, use the **no ip inspect** command in global configuration mode.

no ip inspect

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	11.2 P	This command was introduced.

Usage Guidelines Turn off CBAC with the **no ip inspect** global configuration command.



Note

The **no ip inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults. All existing sessions are deleted and their associated access lists are removed.

Examples The following example turns off CBAC at a firewall:

```
no ip inspect
```

no ip ips sdf builtin

To instruct the router not to load the built-in signatures if it cannot find the specified signature definition files (SDFs), use the **no ip ips sdf builtin** command in global configuration mode.

no ip ips sdf builtin

Syntax Description This command has no arguments or keywords.

Defaults If the router fails to load the SDF, the router will load the default, built-in signatures.

Command Modes Global configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines



Caution

If the **no ip ips sdf builtin** command is issued and the router running Intrusion Prevention System (IPS) fails to load the SDF, you will receive an error message stating that IPS is completely disabled.

Examples

The following example shows how to instruct the router not to refer to the default, built-in signature if the attack-drop.sdf file fails to load:

```
Router(config) no ip ips sdf builtin
```

Related Commands	Command	Description
	copy ips-sdf	Loads or saves the SDF in the router.
	ip ips sdf location	Specifies the location in which the router will load the SDF.

ocsp url

To specify the URL of an online certificate status protocol (OCSP) server to override the OCSP server URL (if one exists) in Authority Info Access (AIA) extension of the certificate, use the **ocsp url** command in ca-trustpoint configuration mode. To disable the OCSP server, use the **no** form of this command.

ocsp url *url*

no ocsp url *url*

Syntax Description	<i>url</i>	All certificates associated with a configured trustpoint will be checked by the OCSP server at the specified HTTP URL.
---------------------------	------------	--

Defaults	Uses the OCSP server URL in AIA extension of the certificate. If a URL does not exist, revocation check will fail.
-----------------	--

Command Modes	Ca-trustpoint configuration
----------------------	-----------------------------

Command History	Release	Modification
	12.3(2)T	This command was introduced.

Usage Guidelines	A central OCSP server can be configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers. Thus, the devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.
-------------------------	---

Examples	The following example shows how to configure your router to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.
-----------------	--

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands	Command	Description
	crypto pki trustpoint	Declares the CA that your router should use.
	revocation-check	Checks the revocation status of a certificate.

outgoing

To configure filtering for outgoing export traffic, use the **outgoing** command in router IP traffic export (RITE) configuration mode. To disable filtering for outgoing traffic, use the **no** form of this command.

outgoing {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

no outgoing {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}

Syntax Description

access-list {*standard* | *extended* | *named*} An existing numbered (standard or extended) or named access control list (ACL).

Note The filter is applied only to exported traffic.

sample one-in-every *packet-number* Export only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets.

Defaults

If this command is not enabled, outgoing IP traffic is not exported.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for IP traffic export, you can issue the **outgoing** command to filter unwanted outgoing traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.



Note

If you issue this command, you must also issue the **bidirectional** command, which enables outgoing traffic to be exported. However, only routed traffic (such as passthrough traffic) is exported; that is, traffic that originates from the network device is not exported.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
```

```
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corpl
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming IP traffic.