



Distinguished Name Based Crypto Maps

Feature History

Release	Modification
12.2(4)T	This feature was introduced.

This feature module describes the Distinguished Name Based Crypto Map feature in Cisco IOS Release 12.2(4)T. It includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 3
- Configuration Examples, page 5
- Command Reference, page 6

Feature Overview

The Distinguished Name Based Crypto Maps feature allows you to configure the router to restrict access to selected encrypted interfaces for those peers with specific certificates, especially certificates with particular Distinguished Names (DNs).

Previously, if the router accepted a certificate or a shared secret from the encrypting peer, Cisco IOS did not have a method of preventing the peer from communicating with any encrypted interface other than the restrictions on the IP address of the encrypting peer. This feature allows you to configure which crypto maps are usable to a peer based on the DN that a peer used to authenticate itself, thereby, enabling you to control which encrypted interfaces a peer with a specified DN can access.

Benefits

The Distinguished Name Based Crypto Maps feature allows you to set restrictions in the router configuration that prevent peers with specific certificates—especially certificates with particular DN—from having access to selected encrypted interfaces.

Restrictions

System Requirements

To configure this feature, your router must support IP Security.

Performance Impact

If you restrict access to a large number of DNSs, it is recommended that you specify a few number of crypto maps referring to large identity sections instead of specifying a large number of crypto maps referring to small identity sections.

Related Documents

The following documents provide information related to the Distinguished Name Based Crypto Maps feature:

- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2

Supported Platforms

This feature is supported on the following platforms:

- Cisco 1700 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 series
- Cisco 7200 series
- Cisco uBR905 Cable Access Router
- Cisco uBR925 Cable Access Router

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Prerequisites

Before configuring a DN based crypto map, you must perform the following tasks:

- Create an Internet Key Exchange (IKE) policy at each peer.

For more information on creating IKE policies, refer to the chapter “Configuring Internet Key Exchange Security Protocol” of the *Cisco IOS Security Configuration Guide*.

- Create crypto map entries for IPSec.

For more information on creating crypto map entries, refer to the chapter “Configuring IPSec Network Security” of the *Cisco IOS Security Configuration Guide*.


Configuration Tasks

See the following sections for configuration tasks for the Distinguished Name Based Crypto Maps feature. Each task in the list is identified as either required or optional.

- Configuring DN Based Crypto Maps (authenticated by DN) (required)
- Configuring DN Based Crypto Maps (authenticated by hostname) (required)
- Applying Identity to DN Based Crypto Maps (required)
- Verifying DN Based Crypto Maps (optional)


Configuring DN Based Crypto Maps (authenticated by DN)

To configure a DN based crypto map that can be used only by peers that have been authenticated by a DN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# crypto identity name</code>	Configures the identity of a router with the given list of DNs in the certificate of the router and enters crypto identity configuration mode.
Step 2	<code>Router(crypto-identity)# dn name=string [,name=string]</code>	Associates the identity of the router with the DN in the certificate of the router.
		 <p>Note The identity of the peer must match the identity in the exchanged certificate.</p>


Configuring DN Based Crypto Maps (authenticated by hostname)

To configure a DN based crypto map that can be used only by peers that have been authenticated by a hostname, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# crypto identity name</code>	Configures the identity of a router with the given list of DNs in the certificate of the router and enters crypto identity configuration mode.
Step 2	<code>Router(crypto-identity)# fqdn name</code>	Associates the identity of the router with the hostname that the peer used to authenticate itself.
		 <p>Note The identity of the peer must match the identity in the exchanged certificate.</p>

Applying Identity to DN Based Crypto Maps

To apply the identity (within the crypto map context), use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto map <i>map-name seq-num</i> ipsec-isakmp	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
Step 2	Router(config-crypto-map)# identity <i>name</i>	Applies the identity to the crypto map. When this command is applied, only the hosts that match a configuration listed within the identity <i>name</i> can use the specified crypto map.
		 <p>Note If the identity command does not appear within the crypto map, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.</p>

Verifying DN Based Crypto Maps

To verify that this functionality is properly configured, use the following command in EXEC mode:

Command	Purpose
Router# show crypto identity	Displays the configured identities.

Troubleshooting Tips

If an encrypting peer attempts to establish a connection that is blocked by the DN based crypto map configuration, the following error message will be logged:

```
<time>: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT: encrypted connection attempted with a peer
without the configured certificate attributes.
```

Configuration Examples

This section provides the following configuration example:

- DN Based Crypto Map Configuration Example

DN Based Crypto Map Configuration Example

The following example shows how to configure DN based crypto maps that have been authenticated by DN and hostname. Comments are included inline to explain various commands.

```
! DN based crypto maps require you to configure an IKE policy at each peer.
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
crypto isakmp policy 20
  authentication pre-share
  lifetime 10000
crypto isakmp key 1234567890 address 171.69.224.33
!
! The following is an IPsec crypto map (part of IPsec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-bigbiz
!
crypto identity to-bigbiz
  dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
  set peer 172.21.115.119
  set transform-set my-transformset
  match address 125
  identity to-little-com
!
crypto identity to-little-com
  fqdn little.com
!
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **crypto identity**
- **dn**
- **fqdn**
- **identity**

crypto identity

To configure the identity of the router with a given list of distinguished names (DNs) in the certificate of the router, use the **crypto identity** command in global configuration mode. To delete all identity information associated with a list of DN, use the **no** form of this command.

crypto identity *name*

no crypto identity *name*

Syntax Description	<i>name</i>	Identity of the router, which is associated with the given list of DN.
---------------------------	-------------	--

Defaults	If this command is not enabled, the IP address is associated with the identity of the router.
-----------------	---

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

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

Usage Guidelines	The crypto identity command allows you to configure the identity of a router with a given list of DN. Thus, when used with the dn and fqdn commands, you can set restrictions in the router configuration that prevent peers with specific certificates, especially certificates with particular DN, from having access to selected encrypted interfaces.
-------------------------	--



Note	The identity of the peer must be the same as the identity in the exchanged certificate.
-------------	---

Examples

The following example shows how to configure a DN based crypto map:

```
! The following is an IPsec crypto map (part of IPsec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-bigbiz
!
crypto identity to-bigbiz
  dn ou=BigBiz
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
  set peer 172.21.115.119
  set transform-set my-transformset
  match address 125
  identity to-little-com
!
crypto identity to-little-com
  fqdn little.com
!
```

Related Commands

Command	Description
dn	Associates the identity of the router with the DN in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

dn

To associate the identity of the router with the distinguished name (DN) in the certificate of the router, use the **dn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

```
dn name=string [, name=string]
```

```
no dn name=string [, name=string]
```

Syntax Description

<i>name=string</i>	Identity used to restrict access to peers with specific certificates. Optionally, you can associate more than one identity.
--------------------	---

Defaults

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

Command Modes

Crypto identity configuration

Command History

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

Usage Guidelines

Use the **dn** command to associate the identity of the router, which is defined in the **crypto identity** command, with the distinguished name that the peer used to authenticate itself.



Note

The *name* defined in the **crypto identity** command must match the *string* defined in the **dn** command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

An encrypting peer matches this list if it contains the attributes listed in any one line defined within the *name=string*.

Examples

The following example shows how to configure an IPsec crypto map that can be used only by peers that have been authenticated by the DN and if the certificate belongs to “BigBiz”:

```
crypto map map-to-bigbiz 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-bigbiz
!
crypto identity to-bigbiz
  dn ou=BigBiz
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

fqdn

To associate the identity of the router with the hostname that the peer used to authenticate itself, use the **fqdn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

fqdn *name*

no fqdn *name*

Syntax Description

name Identity used to restrict access to peers with specific certificates.

Defaults

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

Command Modes

Crypto identity configuration

Command History

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

Usage Guidelines

Use the **fqdn** command to associate the identity of the router, which is defined in the **crypto identity** command, with the distinguished name in the certificate of the router.



Note

The *name* defined in the **crypto identity** command must match the *name* defined in the **fqdn** command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNS, from having access to selected encrypted interfaces.

Examples

The following example shows how to configure a crypto map that can be used only by peers that have been authenticated by hostname and if the certificate belongs to “little.com”:

```
crypto map map-to-little-com 10 ipsec-isakmp
  set peer 172.21.115.119
  set transform-set my-transformset
  match address 125
  identity to-little-com
!
crypto identity to-little-com
  fqdn little.com
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DN's in the certificate of the router.
dn	Associates the identity of the router with the DN in the certificate of the router.

identity

To set the identity to the crypto map, use the **identity** command in crypto map configuration mode.

identity *name*

Syntax Description	<i>name</i> Identity used to permit or restrict access for a host to a crypto map.				
Defaults	If this command is not enabled, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.				
Command Modes	Crypto map configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(4)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(4)T	This command was introduced.
Release	Modification				
12.2(4)T	This command was introduced.				

Usage Guidelines Use the **identity** command to set the identity to the configured crypto maps. When this command is applied, only the hosts that match a configuration listed within the **identity** *name* can use that crypto map.

Examples The following example shows how to configure two IPsec crypto maps and apply the identity to each crypto map. That is, the identity is set to “to-bigbiz” for the first crypto map and “to-little-com” for the second crypto map.

```
! The following is an IPsec crypto map (part of IPsec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-bigbiz
!
crypto identity to-bigbiz
  dn ou=BigBiz
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
  set peer 172.21.115.119
  set transform-set my-transformset
  match address 125
  identity to-little-com
!
crypto identity to-little-com
  fqdn little.com
!
```

Related Commands	Command	Description
	crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
	crypto map	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
	dn	Associates the identity of the router with the DN in the certificate of the router.
	fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.