



Diffie-Hellman Group 5

This document describes the Diffie-Hellman Group 5 feature. It includes information on the benefits of the new feature, supported platforms, related documents, and so on.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 2
- Configuration Tasks, page 3
- Configuration Examples, page 4
- Command Reference, page 4
- Glossary, page 8

Feature Overview

The Diffie-Hellman Group 5 feature enables group 5 on all platforms that support crypto images. Group 5 specifies the 1536-bit Diffie-Hellman group, which is a method of establishing a shared key over an insecure medium.

To specify group 5, you must first enter either the **set pfs** command or the **group** command. The group 5 option works exactly like group 1 and group 2; however, group 5 provides a higher level of security and requires more process time than group 1 and group 2.

Benefits

The 1536-bit Diffie-Hellman group (group 5) provides more security than group 1 and group 2.

Restrictions

The **set pfs** command is available only for ipsec-isakmp crypto map entries and dynamic crypto map entries.

Related Documents

The following documents provide information related to the Diffie-Hellman Group 5 feature:

- *Cisco IOS Security Configuration Guide*, Release 12.1
- *Cisco IOS Security Command Reference*, Release 12.1
- RFC 2412, *The OAKLEY Key Determination Protocol*

Supported Platforms

- Cisco 800 series
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 4000 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 12000 series
- Cisco AS5300 access servers
- Cisco AS5800 access servers
- Cisco c5rsm
- Cisco MC3810 multiservice access concentrators

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on Cisco Connection Online (CCO) at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

- 2412, *The OAKLEY Key Determination Protocol*

Configuration Tasks

See the following sections for configuration tasks for the Diffie-Hellman Group 5 feature. Each task in the list is indicated as optional or required.

- Configuring IKE Policy group 5 (Required)
- Configuring Crypto Map and Specifying PFS with the group 5 option (Optional)

Configuring IKE Policy group 5

To configure an Internet Key Exchange policy with the 1536-bit Diffie-Hellman group (group 5), enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto isakmp policy 25	Defines an IKE policy and enters ISAKMP policy configuration mode.
Step 2	Router(config-isakmp)# group 5	Configures an IKE policy with the 1536-bit Diffie-Hellman group (group 5).
Step 3	Router(config-isakmp)# exit	Exits ISAKMP policy configuration mode.

For more information on creating IKE policies, refer to the chapter “Configuring Internet Key Exchange Security Protocol” in the *Cisco IOS Security Configuration Guide*, Release 12.1.

Configuring Crypto Map and Specifying PFS with the group 5 option

To configure a crypto map and specify that perfect forward secrecy (group 5) should be used whenever a new security association is negotiated for the configured crypto map, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto map mymap 15 ipsec-isakmp	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 2	Router(config-crypto-map)# set pfs group5	(Optional) Specifies that IPsec should ask for perfect forward secrecy when requesting new security associations for this crypto map entry or should demand perfect forward secrecy in requests received from the IPsec peer. In this configuration, IPsec uses the 1536-bit Diffie-Hellman prime modulus group (group 5).
Step 3	Router(config-crypto-map)# exit	Exits crypto map configuration mode.

For more information on creating or modifying crypto map sets, refer to the chapter “Configuring IPsec Network Security” in the *Cisco IOS Security Configuration Guide*, Release 12.1.

Verifying Diffie-Hellman Group 5

To display all existing IKE policies, use the **show crypto isakmp policy** command in EXEC mode.

To view information about your IPsec configuration, use the **show crypto map** command in EXEC mode.

Configuration Examples

This section provides the following configuration examples:

- Configuring an IKE Policy Group 5 Example
- Specifying PFS with the Group 5 Example

Configuring an IKE Policy Group 5 Example

The following example configures an IKE policy with the 1536-bit Diffie-Hellman group (group 5); all other parameters are set to the defaults:

```
crypto isakmp policy 25
  group 5
```

Specifying PFS with the Group 5 Example

The following example specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group (group5) whenever a new security association is negotiated for the crypto map “mymap 15”:

```
crypto map mymap 15 ipsec-isakmp
  set pfs group5
```

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **group (IKE policy)**
- **set pfs**

group (IKE policy)

To specify the Diffie-Hellman group identifier within an IKE policy, use the **group** Internet Security Association and Key Management Protocol (ISAKMP) policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command .

group { **1** | **2** | **5** }

no group

Syntax Description		
	1	The 768-bit Diffie-Hellman group.
	2	The 1024-bit Diffie-Hellman group.
	5	The 1536-bit Diffie-Hellman group.

Defaults 768-bit Diffie-Hellman group (group 1).

Command Modes ISAKMP policy configuration (config-isakmp)

Command History	Release	Modification
	11.3T	This command was introduced.
	12.1(3)T	The keyword 5 was added.

Usage Guidelines Use this command to specify the Diffie-Hellman group to be used in an IKE policy.

Examples The following example configures an IKE policy with the 1024-bit Diffie-Hellman group (group 2); all other parameters are set to the defaults:

```
crypto isakmp policy 15
  group 2
```

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.
	hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
	lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
	show crypto isakmp policy	Displays the parameters for each IKE policy.

set pfs

To specify 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, use the **set pfs** crypto map configuration command. To specify that IPsec should not request PFS, use the **no** form of the command.

set pfs [group1 | group2 | group5]

no set pfs

Syntax Description	group1	(Optional) Specifies that IPsec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
	group2	(Optional) Specifies that IPsec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
	group5	(Optional) Specifies that IPsec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

Defaults By default, PFS is not requested. If no group is specified with this command, **group1** is used as the default.

Command Modes Crypto map configuration

Command History	Release	Modification
	11.3T	This command was introduced.
	12.1(3)T	The group5 keyword was added.

Usage Guidelines This command is available only for **ipsec-isakmp** crypto map entries and dynamic crypto map entries. During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. The default (**group1**) is sent if the **set pfs** statement does not specify a group. If the peer initiates the negotiation and the local configuration specifies PFS, the remote peer must perform a PFS exchange or the negotiation will fail. If the local configuration does not specify a group, a default of **group1** will be assumed, and an offer of either **group1**, **group2**, or **group5** will be accepted. If the local configuration specifies **group2** or **group5**, that group must be part of the offer from the peer or the negotiation will fail. If the local configuration does not specify PFS, it will accept any offer of PFS from the peer.

PFS adds another level of security because if one key is ever cracked by an attacker then only the data sent with that key will be compromised. Without PFS, data sent with other keys could also be compromised.

With PFS, every time a new security association is negotiated, a new Diffie-Hellman exchange occurs. This exchange requires additional processing time.

The 1024-bit Diffie-Hellman prime modulus group, **group2**, provides more security than **group1**, but requires more processing time than **group1**. However, the 1536-bit Diffie-Hellman prime modulus group, **group5**, provides more security than **group1** and **group2**, but requires more processing time than **group1** and **group2**.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto map “mymap 10”:

```
crypto map mymap 10 ipsec-isakmp
 set pfs group2
```

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.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
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 transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

Glossary

crypto map—A Cisco IOS software configuration entity that performs two primary functions: (1) it selects data flows that need security processing, and (2) it defines the policy for these flows and the crypto peer that traffic needs to go to. A crypto map is applied to an interface. The concept of a crypto map was introduced in classic crypto but was expanded for IPSec.

DH—See Diffie-Hellman.

Diffie-Hellman—A public-key cryptography protocol which allows two parties to establish a shared secret over an insecure communications channel. Diffie-Hellman is used within IKE to establish session keys and is a component of Oakley.

Internet Security Association and Key Management Protocol—See ISAKMP.

ISAKMP—Internet Security Association and Key Management Protocol. A protocol framework that defines the mechanics of implementing a key exchange protocol and negotiation of a security policy.

Oakley—A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm.

perfect forward secrecy—See PFS.

PFS—perfect forward secrecy. PFS ensures that a given key of an IPSec security association was not derived from any other secret (like some other keys). In other words, if someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPSec-protected data, and then use knowledge of the IKE SA secret to compromise the IPSec SAs set up by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPSec. The attacker would have to break each IPSec SA individually. Cisco IOS IPSec implementation uses PFS group 1 (DH 768 bit) by default.