ISAKMP Configuration Mode Commands

Modification(s) to an existing ISAKMP policy configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command described in the *Exec Mode (A–C) Commands* chapter for more information.

Command Modes

The ISAKMP Configuration Mode is used to configure Internet Security Association Key Management Protocol (ISAKMP) policies that are used to define Internet Key Exchange (IKE) security associations (SAs).

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands chapter.

authentication

Configures the ISAKMP policy authentication mode.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

Syntax Description

```
authentication preshared-key
[ default | no ] authentication
```

default authentication

Restores the default setting of this parameter. This command is enabled by default.

no authentication

Disables the preshared key authentication mode.

preshared-key

Specifies that the policy will be authenticated through the use of the pre-shared key.

Usage Guidelines

When the system is configured to use ISAKMP-type crypto maps for establishing IPSec tunnels, this command is used to indicate that the policy will be authenticated through the use of the pre-shared key configured in the ISAKMP crypto map.

Example

The following command sets policy authentication mode to use a pre-shared key:

```
authentication preshared-key
```

encryption

Configures the encryption protocol to use to protect subsequent IKE SA negotiations.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

Syntax Description

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc }
[ default | no ] encryption
```

default encryption

Restores the default setting of this parameter.

no encryption

Removes a previously configured encryption type.

3des-cbc

Specifies that the encryption protocol is Triple Data Encryption Standard (3DES) in chain block (CBC) mode.

aes-cbc-128

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.

aes-cbc-256

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.

des-cbc

Specifies that the encryption protocol is DES in CBC mode. This is the default setting.

Usage Guidelines

Once the D-H exchange between the system and the security gateway has been successfully completed, subsequent IKE SA negotiations will be protected using the protocol specified by this command.

Example

The following command sets the IKE encryption method to 3des-cbc:

```
encryption 3des-cbc
```

group

Configures the Oakely group (also known as the Diffie-Hellman [D-H] group) in which the D-H exchange occurs.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > **context** *context_name* > **isakmp policy** *policy_number*

Syntax Description

```
group { 1 | 2 | 5 }
[ default | no ] group
```

default group

Restores the default setting of this parameter.

no group

Removes a previously configured group.

{ 1 | 2 | 5 }

Default: **1**

Specifies the number of the Oakley group. The following groups are allowed:

- **1**: Enables Oakley Group 1 using a 768-bit modp as defined in RFC 2409.
- **2**: Enables Oakley Group 2, using a 1024-bit modp as defined in RFC 2409.
- **5**: Enables Oakley Group 5, using a 1536-bit modp as defined in RFC 3526.

Usage Guidelines

Specifies the Oakley group that determine the length of the base prime numbers that are used during the key exchange process.

Example

The following command sets the group to 5 which specifies 1536-bit base prime numbers:

```
group 5
```

hash

Configures the IKE hash protocol to use during IKE SA negotiations.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator\

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > **context** *context_name* > **isakmp policy** *policy_number*

Syntax Description

```
hash { md5 | sha1 }
[ default | no ] hash
```

default

Restores the default setting of this parameter.

no

Removes a previously configured hash algorithm.

md5

Specifies that the hash protocol is Message Digest 5 truncated to 96 bits.

sha1

Specifies that the hash protocol is Secure Hash Algorithm-1 truncated to 96 bits. This is the default setting for this command.

Usage Guidelines

Use this command to configure the hash algorithm used during key negotiation.

Example

Set the hash algorithm to Message-Digest 5 by entering the following command:

```
hash md5
```

lifetime

Configures the lifetime of the IKE Security Association (SA).

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > **context** *context_name* > **isakmp policy** *policy_number*

Syntax Description

lifetime *seconds*
default lifetime

default lifetime

Restores the default setting of this parameter.

seconds

Default: 86400

The number of seconds for the SA to live. *seconds* must be an integer from 60 to 86400.

Usage Guidelines

Use this command to set the time that an ISAKMP SA will be valid. The lifetime is negotiated with the peer and the lowest configured lifetime duration is used.

Example

The following command sets the SA lifetime to 100 seconds:

lifetime *100*