

IKEv2 Security Association Configuration Mode Commands

The IKEv2 Security Association Configuration Mode is used to configure a Security Association (SA) at the outset of an IPSec session. A security association is the collection of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. In normal bi-directional traffic, the flows are secured by a pair of security associations.

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

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.

- default, on page 1
- encryption, on page 2
- group, on page 3
- hmac, on page 4
- lifetime , on page 6
- prf, on page 6

default

Sets the default properties for the selected parameter.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

default { encryption | group | hmac | lifetime | prf }

Set the defaults for the following parameters:

- **encryption**: Default algorithm for the IKEv2 IKE SA is AES-CBC-128.
- **group**: Default Diffie-Hellman group is Group 2.
- **hmac**: Default IKEv2 IKE SA hashing algorithm is SHA1-96.
- **lifetime**: Default lifetime for SAs derived from this transform-set is 86400 seconds.
- **prf**: Default PRF for the IKEv2 IKE SA is SHA1.

Usage Guidelines

Configure default parameters for the IKEv2 IKE SA transform-set.

Example

Use the following configuration to set the default encryption algorithm:

```
default encryption
```

encryption

Configures the appropriate encryption algorithm and encryption key length for the IKEv2 IKE security association. AES-CBC-128 is the default.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc | null }
default encryption

3des-cbc

Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cypher keys (triple DES).

aes-cbc-128

Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits.

aes-cbc-256

Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.

des-cbc

Data Encryption Standard Cipher Block Chaining. Encryption using a 56-bit key size. Relatively insecure.

null

Configures no IKEv2 IKE Security Association Encryption Algorithm. All IKEv2 IPsec Child Security Association protected traffic will be sent in the clear.



Note USE OF THIS ALGORITHM FOR IKE_SA ENCRYPTION IS A VIOLATION OF RFC 4306. THIS ALGORITHM SHOULD ONLY BE USED FOR TESTING PURPOSES.

Usage Guidelines

IKEv2 requires a confidentiality algorithm to be applied in order to work.

In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly-generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity.

Because RFC 4307 calls for interoperability between IPSec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPSec in order for there to be an acceptable match during the IKE message exchange. Because of RFC4307, in IKEv2, there is no viable NULL option, it is available for testing only.

Example

The following command configures the encryption to be aes-cbc-128:

```
encryption aes-cbc-128
```

group

Configures the appropriate key exchange cryptographic strength by applying a Diffie-Hellman group. Default is Group 2.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

group { 1 | 2 | 5 | 14 }
default group

1

Configures crypto strength at the Group 1 level. Lowest security.

2

Configures crypto strength at the Group 2 (default) level. Medium security.

This is the default setting for this command.

5

Configures crypto strength at the Group 5 level. Higher security.

14

Configures crypto strength at the Group 14 level. Highest security

Usage Guidelines

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process in IKEv2. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.

Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group 14 provides 2048 bits of encryption strength.

Configuring a DH group also enables Perfect Forward Secrecy, which is disabled by default.

Example

This command configures crypto strength at the Group 14 level. Highest security group 14:

default group

hmac

Configures the IKEv2 IKE SA integrity algorithm. Default is SHA1-96.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

hmac { aes-xcbc-96 | md5-96 | sha1-96 | sha2-256-128 | sha2-384-192 | sha2-512-256 }
default hmac

aes-xcbc-96

HMAC-AES-XCBC uses a 128-bit secret key and produces a 128-bit authenticator value.

md5-96

HMAC-MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

sha1-96

HMAC-SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. This is the default setting for this command.

sha2-256-128

HMAC-SHA-256 uses a 256-bit secret key and produces a 128-bit authenticator value.

sha2-384-192

HMAC-SHA-384 uses a 384-bit secret key and produces a 192-bit authenticator value.

sha2-512-256

HMAC-SHA-512 uses a 512-bit secret key and produces a 256-bit authenticator value.

Usage Guidelines

IKEv2 requires an integrity algorithm be configured in order to work.

A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated and transmitted. The authenticator value is reconstituted by the receiver and the first truncated bits are compared for a 100 percent match.

Example

This command configures HMAC value md5-96:

hmac md5-96

lifetime

Configures the lifetime of a security association (SA) in seconds.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

`lifetime` *`sec`*
`default lifetime`

lifetime *sec*

Sets the value of the timeout parameter in seconds as an integer from 60 through 86400. Default: 86400

Usage Guidelines

The secret keys that are used for various aspects of a configuration should only be used for a limited amount of time before timing out. This exposes a limited amount of data to the possibility of hacking. If the SA expires, the options are then to either close the SA and open an new one, or renew the existing SA.

Example

The following command sets the lifetime timeout to 120 seconds:

```
lifetime 120
```

prf

Selects one of the HMAC integrity algorithms to act as the IKE Pseudo-Random Function. A PRF produces a string of bits that an attacker cannot distinguish from random bit string without knowledge of the secret key. The default is SHA1.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

prf { aes-xcbc-128 | md5 | sha1 | sha2-256 | sha2-384 | sha2-512 } default prf

aes-xcbc-128

Configure IKEv2 IKE Security Association Pseudo Algorithm to be AES-XCBC-128.

md5

MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

sha1

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value.

SHA-1 is considered cryptographically stronger than MD5, but it takes more CPU cycles to compute.

This is the default setting for this command.

sha2-256

PRF-HMAC-SHA-256 uses a 256-bit secret key.

sha2-384

PRF-HMAC-SHA-384 uses a 384-bit secret key.

sha2-512

PRF-HMAC-SHA-512 uses a 512-bit secret key.

Usage Guidelines

This command generates keying material for all the cryptographic algorithms used in both the IKE_SA and the CHILD_SAs.

Example

This configuration sets the PRF to be value sha2-256:

```
prf sha2-256
```