

IPSec Transform Set Configuration Mode Commands

The IPSec Transform Set Configuration Mode is used to configure IPSec security parameters. There are two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). AH may be considered redundant as ESP can provide the same authentication services that AH does.

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-context-vrf)#`

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.

- encryption, on page 1
- esn, on page 4
- group, on page 5
- hmac, on page 6
- mode, on page 7

encryption

Configures the appropriate IPSec ESP encryption algorithm and encryption key length. AES-CBC-128 is the default.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

encryption { 3des-cbc | aes-128-gcm-128 | aes-cbc-128 | aes-128-gcm-64 | aes-128-gcm-96 | aes-256-gcm-128 | aes-256-gcm-64 | aes-256-gcm-96 | 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-128-gcm-128

IKEv2 Child Security Association IPsec ESP Algorithm is AES-GCM-128 with 128-bit ICV (Integrity Check Value). HMAC algorithm with this encryption algorithm should be None.

aes-128-gcm-64

IKEv2 Child SA (Security Association) IPsec ESP Algorithm is AES-GCM-128 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-128-gcm-96

IKEv2 Child SA IPsec ESP Algorithm to be AES-GCM-128 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-256-gcm-128

IKEv2 Child SA IPsec ESP Algorithm is AES-GCM-256 with 128-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-256-gcm-64

IKEv2 Child SA IPsec ESP Algorithm is AES-GCM-256 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-256-gcm-96

IKEv2 Child SA IPsec ESP Algorithm is AES-GCM-256 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-cbc-128

Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits. This is the default setting for this command.

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

The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

default

Sets the default IPSec ESP algorithm to AES-CBC-128.

Usage Guidelines

AES-GCM (Advanced Encryption Standard-Galois Counter Mode) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption (RFC 5288). It uses mechanisms that are supported by a well-understood theoretical foundation, and its security follows from a single reasonable assumption about the security of the block cipher. StarOS supports these AEAD (Authenticated Encryption with Associated Data) algorithms for improved IPsec performance when using OpenSSL to process ESP packets.



Important The AEAD algorithms are only supported on virtualized platforms. They are not supported on ASR 5x00 hardware.

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. In IKEv2, there is no NULL option.

Example

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

```
default encryption
```

esn

Enables support for the use of 64-bit Extended Sequence Numbers (ESNs) in ikev2 Encapsulating Security Payload (ESP) and Authentication Header (AH) packets. The ESN transform is included in an ikev2 proposal used in the negotiation of IKE SAs as part of the IKE_SA_INIT exchange.

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

esn

Usage Guidelines

Use this command to enable support for the use of 64-bit ESNs for ikev2. The ESN transform is included in an ikev2 proposal used in the negotiation of IKE SAs as part of the IKE_SA_INIT exchange.

The ESN transform has the following meaning:

- A proposal containing one ESN transform with value 0 means "do not use extended sequence numbers".
- A proposal containing one ESN transform with value 1 means "use extended sequence numbers".
- A proposal containing two ESN transforms with values 0 and 1 means "I support both normal and extended sequence numbers, you choose". This case is only allowed in requests; the response will contain only one ESN transform.

In most cases, the exchange initiator will include either the first or third alternative in its SA payload. The second alternative is rarely useful for the initiator: it means that using normal sequence numbers is not acceptable (so if the responder does not support ESNs, the exchange will fail with NO_PROPOSAL_CHOSEN.

Enabling the **esn** command is the equivalent of sending ESN Transform = 0 and 1; support both 32-bit and 64-bit sequence numbers. If the **esn** command is not enabled, support only 32-bit sequence numbers (default behavior).

Including the ESN transform is mandatory when creating ESP or AH SAs.

For additional information, see the *IPSec Reference*.



Important ESN is only supported on ASR 5500 and ASR 9000 Virtualized Services Modules (VSMs). It is not supported on the ASR 5000 or VPC-SI.

Example

The following command enables support for 64-bit ESNs in ikev2 ESP and AH packets:

esn

group

Configures the appropriate key exchange cryptographic strength and activate Perfect Forward Secrecy by applying a Diffie-Hellman group.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-context-vrf)#`

Syntax Description

`group { 1 | 2 | 5 | 14 | none }`
`default group`

default group

Configures the default crypto strength to be **none** and disables Perfect Forward Secrecy.

1

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

2

Configures crypto strength at the Group 2 level. Medium security.

5

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

14

Configures crypto strength at the Group 14 level. Highest security.

none

Applies no group and disables Perfect Forward Secrecy. This is the default.

default

Sets the default Diffie-Hellman group algorithm to none. This also deactivates PFS.

Usage Guidelines

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process. 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 Group14 2048 bits. Selecting a group automatically activates Perfect Forward Secrecy. The default value is none, which disables PFS

Example

This command configures security at Group 2 and activates PFS:

```
group 2
```

hmac

Configures the IPsec ESP integrity algorithm using a Hash-based Message Authentication Code (HMAC).

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

```
hmac { aes-xcbc-96 | md5-96 | none| null | sha1-96 | sha2-256-128 |
sha2-384-192 | sha2-512-256 }
default hmac
```

default hmac

Sets the default IPSec hashing algorithm to SHA1-96.

aes-xcbc-96

AES-XCBC-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

md5-96

MD5-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

none

Sets the IPsec hashing algorithm to none. Used with OpenSSL AEAD algorithms.

null

Configures the HMAC value to be null. The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

sha1-96

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

HMAC is an encryption technique used by IPsec to make sure that a message has not been altered.

A keyed-Hash-based Message Authentication Code (HMAC), is a type of message authentication code that is 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 to 96 bits and transmitted. The authenticator value is reconstituted by the receiver and the first 96 bits are compared for a 100 percent match.

Example

The following command configures the default HMAC value (SHA1-96):

```
default hmac
```

mode

Configures the security of IP datagrams based on header placement. Tunnel mode applies security to a completely encapsulated IP datagram, while Transport does not. Default is Tunnel mode.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

```
mode { transport | tunnel }
default mode
```

transport

In Transport mode, the IPSec header is applied only over the IP payload, not over the IP header in front of it. The AH and/or ESP headers appear between the original IP header and the IP payload, as follows:

Original IP header, IPSec headers (AH and/or ESP), IP payload (including transport header).

Transport mode is used for host-to-host communications and is generally unsuited to PDIF traffic.

tunnel

In Tunnel mode, the original IP header is left intact, so a complete IP datagram is encapsulated, forming a virtual tunnel between IPSec-capable devices. The IP datagram is passed to IPSec, where a new IP header is created ahead of the AH and/or ESP IPSec headers, as follows:

New IP header, IPSec headers (AH and/or ESP), old IP header, IP payload.

Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-network and host-to-host communications over the Internet.

This is the default setting for this command.

default mode

Sets the default IPSec Mode to Tunnel.

Usage Guidelines

IPSec modes are closely related to the function of the two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). Both of these protocols provide protection by adding to a datagram a header (and possibly other fields) containing security information. The choice of mode does not affect the method by which each generates its header, but rather, changes what specific parts of the IP datagram are protected and how the headers are arranged to accomplish this.

Example

The following command configures the default Tunnel mode:

```
default mode
```