

Crypto IPSec Configuration Mode Commands

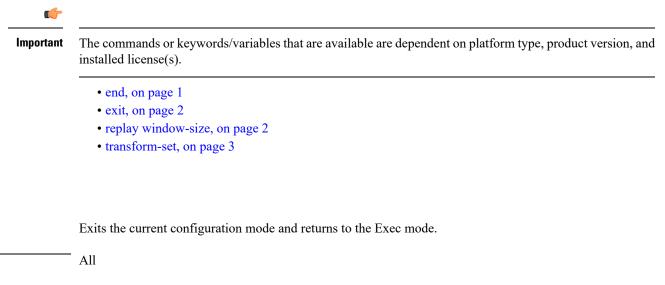
The Crypto IPSec Configuration Mode is used to configure anti-replay window size and properties for system transform sets.

The anti-replay window may be increased to allow the IPSec decryptor to keep track of more than 64 packets.

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Command Modes Exec > Global Configuration > Context Configuration > Crypto IPSec Configuration

configure > context context_name > crypto ipsec



Privilege	Security Administrator, Administrator
Syntax Description	end
Usage Guidelines	Use this command to return to the Exec mode.

end

Product

exit

Exits the current mode and returns to the parent configuration mode.

Product	All
Privilege	Security Administrator, Administrator
Syntax Description	exit
Usage Guidelines	⁻ Use this command to return to the parent configuration mode.

replay window-size

Configures the IPSec anti-replay window size in packets (RFC 6479).

Product	ePDG	
	FA	
	GGSN	
	НА	
	HeNBGW	
	HNBGW	
	HSGW	
	MME	
	P-GW	
	PDSN	
	S-GW	
	SAEGW	
	SCM	
	SecGW	
	SGSN	
Privilege	Security Administrator	
Syntax Description	replay window-sizewindow_size	
	window_size	

Specifies the size of the anti-replay window in packets. Enter one of the following integers to change the number of packets in the window: 32, 64 (default), 128, 256, 384, 512.

Increasing the anti-replay window size has no impact on throughput and security.

Usage Guidelines

IPSec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. This CLI command allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Example

The following command specifies an IPSec anti-replay window size of 128 packets.

crypto ipsec replay window-size 128

transform-set

Configures a transform set for IPSec policy

Product	ePDG
	FA GGSN HA HeNBGW HNBGW HSGW MME P-GW PDSN S-GW SAEGW
	SecGW
	SGSN
Privilege	Security Administrator, Administrator

tran_set_name

Specifies the name of the transform set as an alphanumeric stgring of 1 through 127 characters.

ah hmac { md5-96 | sha1-96 }

Specifies the use of Authentication Header (AH) with a hash-based message authentication code (HMAC) to guarantee connectionless integrity and data origin authentication of IP packets.

Hash options are MD5 Message-Digest Algorithm (md5-96) or Secure Hash Standard 1 (sha1-96).

esp hmac { md5-96 | none | sha1-96 }

Specifies the use of Encapsulating Security Payload (ESP) with a hash-based message authentication code (HMAC) to guarantee connectionless integrity and data origin authentication of IP packets.

Hash options are MD5 Message-Digest Algorithm (md5-96), no hash, or Secure Hash Standard 1 (sha1-96).

cipher

If ESP is enabled, this option must be used to set the encapsulation cipher protocol to one of the following:

- 3des-cbc: Triple Data Encryption Standard (3DES) in chain block (CBC) mode.
- aes-cbc-128: Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.
- aes-cbc-256: Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.
- des-cbc: DES in CBC mode.
- **Usage Guidelines** Use this command to configure a transform set that specifies the type of IPSec protcol to use for securing communications.

Example

The following command specifies the use of IPSec AH with HMAC = MD5.

crypto ipsec transform-set tset013 ah hmac md5-96