

IPsec Extended Sequence Number

The Extended Sequence Number (ESN) is an addition to the IPsec standard sequence number that is used to assist high-speed IPsec implementations. IPSec packets have 32 bit sequence numbers, and rekey is mandatory for IKE-keyed IPSec Security Association (SA) after a sequence number rollover. ESN attempts to reduce this high IPsec SA rekey rate by extending the sequence number to 64 bits, this would increase the time before mandatory rekeys.

- Prerequisites for IPsec Extended Sequence Number , on page 1
- Restrictions for IPsec Extended Sequence Number , on page 1
- **Information About IPsec Extended Sequence Number**, on page 2
- How to Configure IPsec Extended Sequence Number, on page 2
- Additional References, on page 3
- Feature Information for IPsec ESN support , on page 3

Prerequisites for IPsec Extended Sequence Number

- ESN must be supported by both IPsec peers involved in establishing a secure connection. This feature will not function if either one of the peers does not support ESN
- Anti-replay configuration is required, when using ESN. For more details see, IPsec Anti-Replay Window Expanding and Disabling.

Restrictions for IPsec Extended Sequence Number

- ESN is only supported on Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series ESP 100-X and ESP 200-X.
- ESN feature is not supported with DES or 3DES algorithms.

Information About IPsec Extended Sequence Number

IPsec Extended Sequence Number

The Extended Sequence Number (ESN) is an addition to the IPsec standard sequence number that is used to assist high-speed IPsec implementations. ESN uses a larger sequence number space than the standard sequence number and it allows the customer to transmit large volumes of data at a high speed without rekeying.

IPSec packets have 32 bit sequence numbers, and rekey is mandatory for IKE-keyed IPSec Security Association (SA) after a sequence number rollover. ESN attempts to reduce this high IPsec SA rekey rate by extending the sequence number to 64 bits, this would increase the time before mandatory rekeys and prevents sequence number rollover. As a result, it lowers the usage of system resources and prevents frequent rekeying on high speed IPsec connections or IPsec implementations that require long IPsec SA lifetime.

How to Configure IPsec Extended Sequence Number

Configuring IPsec Extended Sequence Number

To configure IPsec Extended Sequence Number support, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*]
4. **esn**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*]	Configures Transform Sets for IPsec.

	Command or Action	Purpose
	Example: `Router (config)# crypto ipsec transform-set foo esp-aes esp-sha-hmac`	• There are complex rules defining the entries that you can use for transform arguments. These rules are explained in the command description for the **crypto ipsec transform-set** command, and the table in "About Transform Sets" section provides a list of allowed transform combinations.
Step 4	**esn** **Example:** `Router(cfg-crypto-trans)#[no] esn [optional]`	(Optional) Enables IPsec ESN.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Security Command Reference

Feature Information for IPsec ESN support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for IPsec Extended Sequence Number

Feature Name	Releases	Feature Information
IPsec Extended Sequence Number (ESN)	Cisco IOS XE Gibraltar 16.11.1 release	This feature was introduced for the following platforms: • Cisco Catalyst 8500 Series Edge Platforms • Cisco ASR 1000 Series ESP 100-X and ESP 200-X

Feature Name	Releases	Feature Information
IPsec Extended Sequence Number (ESN)	Cisco IOS XE Release 17.18.x	This feature was introduced for the following platforms: • Cisco 8200 Series Secure Routers • Cisco 8300 Series Secure Routers • Cisco 8400 Series Secure Routers • Cisco 8500 Series Secure Routers • Cisco 8600 Series Secure Routers