ANSSI Enhancements for IKEv1 and IKEv2 ACL Modes

From Release 20 onwards, the ANSSI for ACL modes have been enhanced to provide additional functionalities.

The following topics are discussed:

Feature Description

The ANSSI for ACL modes have been enhanced with the following functionalities:

Auto-delete Existing IKEv1/IKEv2 ACL Tunnels

IPSec will automatically remove existing IKEv1/IKEv2 ACL Tunnels when the following critical parameters are changed in the crypto map:

- When the IPSec or IKE algorithms change in the IPSec/IKE transform set. For example, Encryption, Integrity, PRF, or DH Group algorithms.
- When authentication methods like PSK/Cert change locally or remotely.
- When the PSK keys change.
- When the certificate, CA-Cert list or CA-CRL list changes.
- When a peer address is changed or removed.
- When the transform set in the crpyto-map is changed or removed.
- When an ACL rule that is added or deleted in the existing ACL which is attached to the map.
- When an ACL is removed from the map.
- When an ACL which is attached to the map is deleted.

- [IKEv1 only] When changes occur in the crypto group.
- [IKEv1 only] When changes occur to the IP-Pool which is associated to the crypto map.
- [IKEv1 only] When changes occur to the IKEv1 policy or policy parameters.

Important Critical parameter changes inside the IKEv1 policy will delete all the established tunnels within that context.

Remove Weak Security Algorithms

The following algorithms are considered weak and removed from the IPSec IKEv2 ACL mode:

IKE Tunnel	Encryption	DES-CBC, 3DES-CBC, NULL
	HMAC	AES-XCBC-96, MD5-96, SHA1-96
	DH Group	1, 2
	PRF	AES-XCBC-128, MD5, SHA1
IPSec Tunnel	Encryption	DES-CBC, 3DES-CBC, NULL
	HMAC	AES-XCBC-96, MD5-96, SHA1-96
	DH Group	1, 2, none

The following algorithms are considered weak and removed from the IPSec IKEv1 ACL mode:

IKE Tunnel	Encryption	DES-CBC, 3DES-CBC
	HMAC	MD5
	DH Group	1, 2
IPSec Tunnel	Encryption	DES-CBC, 3DES-CBC
	HMAC	MD5-96, none
	DH Group	1, 2

Configuring ANSSI Enhancements

Enabling Auto-deletion of Existing IKEv1/IKEv2 ACL Tunnels

Use the **ikesa delete on-mismatch** command to enable IPSec to automatically remove existing IKEv1 and IKEv2 ACL tunnels when critical parameters are changed in the crypto map.

```
configure
   ikesa delete on-mismatch
   end
```

Notes:

- As per ANSSI standards, this configuration cannot be removed once enabled. The configuration can be removed only by rebooting.
- Use this configuration only on trusted builds.