Configuring Transform Sets for IKEv1 and IKEv2 Proposals

Perform this task to define a transform set that is to be used by the IPsec peers during IPsec security association negotiations with IKEv1 and IKEv2 proposals.

- Configuring Transform Sets for IKEv1, on page 1
- Configuring Transform Sets for IKEv2, on page 2
- Verifying Transform Sets for IKEv1, on page 3
- Verifying Transform Sets for IKEv2, on page 3

Configuring Transform Sets for IKEv1

Only tunnel mode is supported.

```
enable
crypto ipsec
transform-set aesset esp-aes 256 esp-sha-hmac
mode tunnel
end
```

**Optional Configurations**

Use the `clear crypto sa` command to clear existing IPsec associations in a transform set.

```
Router # clear crypto sa ?
counters Reset the SA counters
map Clear all SAs for a given crypto map
peer Clear all SAs for a given crypto peer
spi Clear SA by SPI
vrf VRF (Routing/Forwarding) instance
```

There are complex rules defining the entries that you can use for transform arguments. These rules are explained in the `crypto ipsec transform-set` command. For more information, see About Transform Sets.
Configuring Transform Sets for IKEv2

enable
configure terminal
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
mode tunnel
crypto ikev2 proposal proposal-1
encryption aes-cbc-128
integrity sha1
group 14
end

Transform Sets for IKEv2 Examples

The following examples show how to configure a proposal:

**IKEv2 Proposal with One Transform for Each Transform Type**

Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128
Device(config-ikev2-proposal)# integrity sha1
Device(config-ikev2-proposal)# group 14

**IKEv2 Proposal with Multiple Transforms for Each Transform Type**

crypto ikev2 proposal proposal-2
encryption aes-cbc-128 aes-cbc-192
integrity sha1 sha256
group 14 15

For a list of transform combinations, see Configuring Security for VPNS with IPsec.

**IKEv2 Proposals on the Initiator and Responder**

The proposal of the initiator is as follows:

Device(config)# crypto ikev2 proposal proposal-1
Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-196
Device(config-ikev2-proposal)# integrity sha1 sha256
Device(config-ikev2-proposal)# group 14 16

The proposal of the responder is as follows:

Device(config)# crypto ikev2 proposal proposal-2
Device(config-ikev2-proposal)# encryption aes-cbc-196 aes-cbc-128
Device(config-ikev2-proposal)# integrity sha256 sha1
Device(config-ikev2-proposal)# group 16 14

In the scenario, the initiator’s choice of algorithms is preferred and the selected algorithms are as follows:

encryption aes-cbc-128
integrity sha1
group 14
Verifying Transform Sets for IKEv1

Router# show crypto ipsec transform-set

Transform set default: { esp-aes esp-sha-hmac }
 will negotiate = { Transport, },

Transform set ESP-AES256-SHA1: { esp-256-aes esp-sha-hmac }
 will negotiate = { Tunnel, },

Transform set ESP-SHA384-HMAC_504: { esp-des esp-sha384-hmac }
 will negotiate = { Tunnel, },

Transform set ESP-SHA384-HMAC_30: { esp-des esp-sha384-hmac }
 will negotiate = { Tunnel, },

Transform set AES-SHA1: { esp-aes esp-sha-hmac }
 will negotiate = { Tunnel, },

Transform set ab: { esp-aes esp-sha512-hmac }
 will negotiate = { Tunnel, },

Verifying Transform Sets for IKEv2

Router# show crypto ikev2 proposal
IKEv2 proposal: 30
 Encryption: 3DES
 Integrity: SHA96
 PRF: SHA1
 DH Group: DH_GROUP_2048_MODP/Group 14

IKEv2 proposal: default
 Encryption: AES-CBC-256 AES-CBC-192 AES-CBC-128
 Integrity: SHA512 SHA384 SHA256 SHA96 MD596
 PRF: SHA512 SHA384 SHA256 SHA1 MD5
 DH Group: DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2

IKEv2 proposal: prop1
 Encryption: AES-CBC-128
 Integrity: MD596
 PRF: MD5
 DH Group: DH_GROUP_2048_MODP/Group 14
Verifying Transform Sets for IKEv2