IPSec Commands

This module describes the commands used to configure IPSec.

The IPSec and IKEv2 commands apply to the below listed Cisco NCS 540 series routers only:

- N540X-12Z16G-SYS-D
- N540X-12Z16G-SYS-A

ikev2 policy

To configure any parameters for the Internet Key Exchange Version 2 (IKEv2) policy, use the **ikev2 policy** command in XR Config mode.

ikev2 policy *name* { **match** { **address local** *address* | **vrf** { *name* | **any** } } | **proposal** *name* }

Syntax Description

name	Specifies the name for the IKEv2 policy
match	Specifies that a match type follows
address local *address*	Specifies the ip address of the local interface to be associated with this IKEv2 profile
vrf	Configures VRF profile for the IKEv2 policy.
name	Specifies the name of the dedicated VRF profile
any	Specifies that the IKEv2 policy can use any matching VRF profile in the router.
proposal *name*	Specifies the IKEv2 proposal for the IKEv2 policy

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

Before configuring IKEv2 policy, an IKEv2 proposal must be available in your router.

Examples

This example shows how to create a IKEv2 policy:

```
RRouter# configure
Router (config)# ikev2 policy ikev2_policy_P2 match address local 5.22.16.52
Router (config)# ikev2 policy ikev2_policy_P2 match fvrf any
Router (config)# ikev2 policy ikev2_policy_P2 proposal ikev2_proposal_P1
Router (config)# commit
```

ikev2 profile

To configure the parameters of an Internet Key Exchange Version 2 (IKEv2) profile, use the **ikev2 profile** command in XR Config mode.

ikev2 profile name { **keyring ppk name** | **lifetime seconds** | **match** { **fvrf** { **name** | **any** } | **identity remote** } | **authentication** { **local** | **remote** } { **pre-shared** | **rsa-signature** } | **pki trustpoint name** }

Syntax Description

name	Specifies the name of the IKEv2 profile
`keyring` *name*	Configures the trustpoints used for user certificate validation
`keyring ppk`	(Optional) When configured, PPK related IKEv2 packet exchange is enabled.
lifetime *seconds*	Specifies the name of the trustpoint
match	Specifies that a match type follows
fvrf	Configures the FVRF profile for the IKEv2 profile.
name	Specifies the name of the dedicated FVRF profile.
any	Specifies that the IPSec profile can use any matching FVRF profile in the router.
authentication	Specifies that the IPSec Peer authentication method follows
local	Specifies that the authentication occurs on the source router.
remote	Specifies that the authentication occurs on the peer router.
pre-shared	Specifies that the authentication uses the pre-shared key available in the router
rsa-signature	Specifies that the authentication is X.509v3 certificate based on rsa signature
identity remote	Specifies that the identity match for the IKEv2 profile is via the remote identity
`pki trustpoint` *name*	Specifies the public key infrastructure trustpoint name in the IPSec profile

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.
Release 24.1.1	The **keyring ppk** keyword is introduced in the **ikev2 profile** command.

Usage Guidelines

Before creating an IKEv2 profile, A keyring profile must be available in your router.

This example shows how to configure an IKEv2 profile:

```
Router#configure
Router(config)# ikev2 profile ikev2_prof_mgmt_P1 keyring key_mgmt_P1
Router(config)# ikev2 profile ikev2_prof_mgmt_P1 lifetime 600
Router(config)# ikev2 profile ikev2_prof_mgmt_P1 match identity remote address 5.22.16.25
255.255.0.0
Router(config)#commit
```

This example shows how to configure dynamic PPK for one or more peers or groups of peers, in the IKEv2 keyring.

```
Router#configure terminal
Router(config)#keyring dynamic
Router(config-ikev2-keyring)#peer peer1
Router(config-ikev2-keyring-peer)#ppk dynamic qkd required
Router(config-ikev2-keyring)#pre-shared-key cisco123!cisco123
Router(config-ikev2-keyring-peer)#address 10.0.0.1 255.0.0.0
Router(config)#ikev2 profile test
Router(config-ikev2-profile-test)#keyring dynamic
Router(config-ikev2-profile-test)#keyring ppk dynamic
Router(config-ikev2-profile-name)#match address 10.0.0.1 255.255.255.0
Router(config)#sks profile qkd type remote
Router(config-sks-profile)#kme server ipv4 192.0.2.34 port 10001
Router(config-ikev2-keyring-peer)#exit
Router(config)#exit
```

ikev2 proposal

To configure the parameters for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **ikev2 proposal** command in XR Config mode.

ikev2 proposal *name* { **dh-group** { **19** | **20** | **21** } | **encryption** { **aes-gcm-128** | **aes-gcm-256** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** } | **integrity** { **sha-1** | **sha-256** | **sha-384** | **sha-512** } | **prf** { **sha-1** | **sha-256** | **sha-384** | **sha-512** } }

Syntax Description

name	Specifies the name for the IKEv2 proposal
dh-group	Specifies that the transform of the DH group follows. **Note** You can configure one or more DH groups by separating them by a comma.
19	Specifies the ECP group type DH Group-19 (256-bit)
20	Specifies the ECP group type DH Group-20 (384-bit)
21	Specifies the ECP group type DH Group-21 (512-bit)
encryption	Specifies that the type of encryption algorithm follows. **Note** You can configure one or more encryption algorithms by separating them by a comma.
aes-gcm-128	Specifies 128 bits encryption using the Advanced Encryption Standard (AES) with Galois/Counter Mode (AES-GCM).
aes-gcm-256	Specifies 256 bits encryption using the Advanced Encryption Standard (AES) with Galois/Counter Mode (AES-GCM).
aes-cbc-128	Specifies 128 bits encryption using the Advanced Encryption Standard (AES) with cipher-block chaining (CBC).
aes-cbc-192	Specifies 192 bits encryption using the Advanced Encryption Standard (AES) with cipher-block chaining (CBC).
aes-cbc-256	Specifies 256 bits encryption using the Advanced Encryption Standard (AES) with cipher-block chaining (CBC).
integrity	Specifies that the type of algorithm used to authenticate packets in IPSec follows. **Note** You can configure one or more integrity algorithms by separating them by a comma.
sha-1	Specifies that SHA-1 algorithm is used to authenticate in IPSec packets.
sha-256	Specifies that SHA-256 algorithm is used to authenticate in IPSec packets.
sha-384	Specifies that SHA-384 algorithm is used to authenticate in IPSec packets.

sha-512	Specifies that SHA-512 algorithm is used to authenticate in IPSec packets.
prf	Specifies the type of algorithm used to provide randomness for keying information in IPSec follows. **Note** You can configure one or more PRF algorithms by separating them by a comma.
sha-1	Specifies that SHA-1 algorithm is used to provide randomness for keying information.
sha-256	Specifies that SHA-256 algorithm is used to provide randomness for keying information.
sha-384	Specifies that SHA-384 algorithm is used to provide randomness for keying information.
sha-512	Specifies that SHA-512 algorithm is used to provide randomness for keying information.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

This example shows how to configure a IKEv2 profile:

```
Router# configure
Router(config)# ikev2 proposal ikev2_proposal_P1 prf sha-256
Router(config)# ikev2 proposal ikev2_proposal_P1 dh-group 20
Router(config)# ikev2 proposal ikev2_proposal_P1 integrity sha-256
Router(config)# ikev2 proposal ikev2_proposal_P1 encryption aes-cbc-256
Router(config)# commit
```

ipsec profile

To create an IPSec profile, use the **ipsec profile** command in XR Config mode.

ipsec profile *name* **set** { **ikev2-profile** *name* | **pfs** { **group19** | **group20** | **group21** } | **security-association lifetime** *seconds* | **transform-set** *name* | **responder-only** }

Syntax Description

name	Specifies the name for the IPSec profile
ikev2-profile *name*	Associates the specified IKEv2 profile with the IPSec profile.
pfs	Specifies that a DH group follows.
group19	Specifies the MODP group type DH Group1 (768-bit).
group20	Specifies the MODP group type DH Group2 (1024-bit).
group21	Specifies the MODP group type DH Group5 (1536-bit).
security-association lifetime *seconds*	Configures the duration of the security associations (SA) validity in seconds. The security association lifetime value ranges between 120-2592000 seconds. The default value of the fixed lifetime associated with SA is 14400 seconds.
transform-set *name*	Associates the specified transform set with the IPSec profile.
responder-only	Allows a router configured with this command to respond to an initiation request from an IPSec peer router. The router cannot initiate an IPSec session.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.
Release 7.11.1	The **responder-only** keyword was introduced.

Usage Guidelines

Before creating an IPSec profile, an IKEv2 profile and transform set must be available in your router.

Examples

The following example iterates how to create an IPSec profile:

```
Router# config
Router(config)# ipsec profile set ikev2 profile ikev2_prof_mgmt_P2
Router(config)# ipsec profile set pfs group19
Router(config)# ipsec profile set security-association lifetime seconds 14400
Router(config)# ipsec profile set transform-set ts_mgmt_P2
Router (config)# ipsec profile set responder-only
```

```
Router(config)# commit
```

ipsec transform-set

To configure the transform set parameters of an IPSec profile, use the **ipsec transform-set** command in XR Config mode.

ipsec transform-set *name* { **mode tunnel** | **tansform** { **esp-192-aes** | **esp-256-aes** | **esp-hmac-sha-256** | **esp-hmac-sha-384** | **esp-hmac-sha-512** | **esp-hmac-sha1** } }

Syntax Description

name	Specifies the name for the transform set.
mode	Species that the IPSec channel type follows.
tunnel	Specifies the IPSec channel between the interfaces is a tunnel.
transform	Specifies that the algorithm used in the transform set follows.
esp-192-aes	Specifies that the transform set uses the ESP-192-AES algorithm for encryption.
esp-256-aes	Specifies that the transform set uses the ESP-256-AES algorithm for encryption.
esp-hmac-sha-256	Specifies that the transform set uses the ESP-HMAC-SHA-256 algorithm for encryption.
esp-hmac-sha-384	Specifies that the transform set uses the ESP-HMAC-SHA-384 algorithm for encryption.
esp-hmac-sha-512	Specifies that the transform set uses the ESP-HMAC-SHA-512 algorithm for encryption.
esp-hmac-sha1	Specifies that the transform set uses the ESP-HMAC-SHA1 algorithm for encryption.

Command Default

No specific guidelines impact the use of this command.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure an IPSec transform set:

```
Router#configure
Router(config)# ipsec transform-set ts_mgmt_P2 mode tunnel
Router(config)# ipsec transform-set ts_mgmt_P2 transform esp-hmac-sha-256
Router(config)#commit
```

keyring

To configure the keying details of an IPSec profile, use the **keyring** command in XR Config mode.

keyring *name* **peer** **ppk** { **manual** | **dynamic** } *name* { **address** *ip* | **pre-shared-key** { **clear** | **local** | **password** } *key* }

Syntax Description

keyring *name*	Specifies the name for the keyring profile
peer *name*	Specifies the name of the peer interface
ppk manual/dynamic	Provision the same PPK on both IKEv2 and IPsec initiator and responder manually or dynamically from an external key source.
address *ip*	Specifies the ip address of the peer interface along with the prefix.
clear	Specifies that the preshared key for IPSec communication is in cleartext format.
local	Specifies that the preshared key for IPSec communication is a local passphrase.
password	Specifies that the preshared key for IPSec communication is an encrypted string in hexadecimal format.
key	Specifies the preshared key for IPSec communication.

Command Default

No specific guidelines impact the use of this command.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.
Release 24.1.1	The **ppk manual/dynamic** keyword was introduced in the **keyring** command.

Usage Guidelines

None

Examples

This example shows how to configure the keyring parameters for IPSec:

```
Router# config
Router(config)# keyring key_mgmt_P1 peer ACADIA-2 address 5.22.16.25 255.255.0.0
Router(config)# keyring key_mgmt_P1 peer ACADIA-2 pre-shared-key cisco123
Router(config)# commit
```

This example shows how to configure the manual PPK for one or more peers or groups of peers, in the IKEv2 keyring.

```
Router#configure terminal
Router(config)#keyring manual
Router(config-ikev2-keyring)#peer peer1
Router(config-ikev2-keyring-peer)#ppk manual id cisco123 key password 060506324F41584B56
required
Router(config-ikev2-keyring)#pre-shared-key cisco123!cisco123
Router(config-ikev2-keyring-peer)#address 10.0.0.1 255.0.0.0
Router(config)#ikev2 profile test
Router(config-ikev2-profile-test)#keyring manual
Router(config-ikev2-profile-test)#keyring ppk manual
Router(config-ikev2-profile-name)#match address 10.0.0.1 255.255.255.0
Router(config-ikev2-keyring-peer)#exit
Router(config)#exit
```

Examples

This example shows how to configure the dynamic PPK for one or more peers or groups of peers, in the IKEv2 keyring.

```
Router#configure terminal
Router(config)#keyring dynamic
Router(config-ikev2-keyring)#peer peer1
Router(config-ikev2-keyring-peer)#ppk dynamic qkd required
Router(config-ikev2-keyring)#pre-shared-key cisco123!cisco123
Router(config-ikev2-keyring-peer)#address 10.0.0.1 255.0.0.0
Router(config)#ikev2 profile test
Router(config-ikev2-profile-test)#keyring dynamic
Router(config-ikev2-profile-test)#keyring ppk dynamic
Router(config-ikev2-profile-name)#match address 10.0.0.1 255.255.255.0
Router(config)#sks profile qkd type remote
Router(config-sks-profile)#kme server ipv4 192.0.2.34 port 10001
Router(config-ikev2-keyring-peer)#exit
Router(config)#exit
```

show ikev2 session detail

To view details of IKEv2 sessions in your router, use the **show ikev2 session detail** command in XR EXEC mode.

show ikev2 session detail

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

This example shows the usage of **show ikev2 session detail** command:

```
Router#RP/0/RP0/CPU0:R1#show platform security integrity statistics ima-cache block stats
RP/0/RP0/CPU0:ios# show ikev2 session detail
Session ID                              : 1
==========================================================
 Status                                 : UP-ACTIVE
 IKE Count                              : 1
 Child Count                            : 1
 IKE SA ID                              : 1
-------------------------------------------------------------------------------------------
  Local                                : 1.1.1.1/500
  Remote                               : 1.1.1.2/500
  Status(Description)                  : READY (Negotiation done)
  Role                                 : Initiator
  Encryption/Keysize                   : AES-CBC/128
  PRF/Hash/DH Group                    : SHA1/SHA256/20
  Authentication(Sign/Verify)          : PSK/PSK
  Authentication(Sign/Verify)          : RSA/RSA (for certificate based)
  Life/Active Time(sec)                : 86400/2043
  Session ID                           : 1
  Local SPI                            : 3B95C7FCC6A69D0A
  Remote SPI                           : F44C4DBCFEE67F07
  Local ID                             : 1.1.1.1
  Remote ID                            : 1.1.1.2

 Child SA
-------------------------------------------------------------------------------------------
   Local Selector                      : 1.1.1.1/1000 - 1.1.1.1/1000
   Remote Selector                     : 1.1.1.2/1000 - 1.1.1.2/1000
   ESP SPI IN/OUT                      : 0x6c7b15b7 / 0xbf55acd7
   Encryption                          : AES-GCM
   Keysize                             : 256
   ESP HMAC                            : None
```

show ikev2 session

To display the statistics of an IKEv2 session in thr router, use the **show ikev2 session** command in XR EXEC mode.

show ikev2 session

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

This example shows the sample output of the **show ikev2 session** command:

```
Router# show ikev2 session
Session ID               : 1
===================================
Status                   : UP-ACTIVE
IKE Count                : 1
Child Count              : 1
IKE SA ID                : 1
---------------------------------------------------
Local                    : 1.1.1.1/500
Remote                   : 1.1.1.2/500
Status(Description)      : READY (Negotiation done)
Role                     : Initiator
Child SA
----------------------------------------------
Local Selector             : 1.1.1.1/1000 - 1.1.1.1/1000
Remote Selector            : 1.1.1.2/1000 - 1.1.1.2/1000
ESP SPI IN/OUT             : 0x6c7b15b7 / 0xbf55acd7
```

show ikev2 summary

To display the IKEv2 session summary of your router, use the **show ikev2 summary** command in XR EXEC mode.

show ikev2 summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

This example shows the sample output of the **show ikev2 summary** command:

```
Router# show ikev2 summary
IKEv2 Session Summary
-------------------------------------------------
Total Sa (Active/Negotiation)         : 2 (1/1)
Total Outgoing Sa (Active/Negotiation): 2 (1/1)
Total Incoming Sa (Active/Negotiation): 0 (0/0)
```

show ipsec sa

To display the Security Association (SA) details of the interfaces used for IPSec in the router, use the **show ipsec sa** command in the XR EXEC mode.

show ipsec sa [**interface** *name*]

Syntax Description

interface	Specifies that an interface name follows
name	Specifies the name of the interface for which the displays the IPSec Security-Association (SA)

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Examples

The following sample output is from the **show ipsec sa** command:

```
Router# show ipsec sa
If/name             SA-Id   Inbound SPI   Outbound SPI
---------------------------------------------------------
tunnel-ip1          804     0x2c378849    0xa9ed8828
```

```
Router# show ipsec sa interface tunnel-ip1
-------------------------------------
Interface Name      : tunnel-ip1
Interface handle    : 0x800090
SA id               : 713
Mode                : Tunnel
-------------------------------------
Inbound SA
SPI                   : 0xab487871
Protocol              : ESP
Encrypt Algorithm     : ESP_192_AES
Auth Algorithm        : HMAC_SHA_256
Rekey (After Seconds) : 37
-------------------------------------
Outbound SA
SPI                  : 0x1488529e
Protocol             : ESP
Encrypt Algorithm    : ESP_192_AES
Auth Algorithm       : HMAC_SHA_256
Rekey (After Seconds): 37
```