IKEv2 Mobility and Multi-homing Protocol

This chapter provides information on the IKEv2 Mobility and Multi-homing Protocol feature.

The following topics are discussed:

Feature Description

Overview

IPSec can support IKEv2 Mobility and Multi-homing protocol (MOBIKE) as defined in *RFC 4555*. IKEv2 Mobility and Multi-homing Protocol (MOBIKE) allows the IP addresses associated with IKEv2 and tunnel mode IPSec Security Associations (SA) to change. A mobile Virtual Private Network (VPN) client could use MOBIKE to keep the connection with the VPN gateway active while moving from one address to another. Similarly, a multi-homed host could use MOBIKE to move the traffic to a different interface if, for instance, the one currently being used stops working. This enables peer hosts to change its point of network attachment and use different interfaces without removing the existing IPSec tunnel.

The MOBIKE feature is suited when the address of at least one peer is stable, and can be discovered using mechanisms such as DNS. While both parties can be mobile, one party must be rooted at any given time. Additionally, the Gateway is neither multi-homed nor possess mobility capabilities.

Supported Platforms

Currently, IPSec supports the MOBIKE feature on Cisco ASR 5500 and Ultra Services platforms.

How IKEv2 Mobility and Multi-homing Protocol Works

Signaling

MOBIKE is initiated when the feature is enabled, and the Gateway receives an IKE_AUTH containing the SA payload with MOBIKE_SUPPORTED from the peer. The Gateway responds with an IKE_AUTH containing the SA payload with MOBIKE_SUPPORTED.

The feature can be enabled using the **ikesa mobike** command under the Crypto Template Configuration Mode. For more information on the **ikesa mobike** command, refer Enabling IKEv2 Mobility and Multi-homing Protocol, on page 3.

Return Routability Check

A return routability check ensures that the other party can receive packets at the claimed address. When the Gateway receives an UPDATE_SA_ADDRESS, IKE SA/IPSec SA is updated and return routability check is triggered. This function can be enabled using the **ikesa mobike cookie-challenge** command under the Crypto Template Configuration Mode. By default, the Gateway does not perform the return routability check. When enabled, the Gateway sends a cookie challenge to the peer. The session is deleted when a response is not received, or when an invalid response is received. It is assumed that when a valid response is received for any informational exchange, the peer can receive packets at the claimed address.

For more information on the **ikesa mobike cookie-challenge** command, refer Enabling IKEv2 Mobility and Multi-homing Protocol, on page 3.

To ensure that the peer cannot generate the correct INFORMATIONAL response without seeing the request, a new payload is added to INFORMATIONAL messages. The sender of an INFORMATIONAL request can include a COOKIE2 notification, and if included, the recipient of an INFORMATIONAL request copies the notification as-is to the response. When processing the response, the original sender verifies that the value is the same as sent. If the values do not match, the IKE_SA is closed.

Limitations and Restrictions

This section identifies limitations and restrictions for the MOBIKE feature:

- Mobility is supported for peers only. The Gateway has a fixed interface/IP and does not move across the network.
- IPSec supports MOBIKE for Subscriber mode only.
- When a change of address occurs, the peers must always notify the change to the Gateway.
- As the Gateway has a single IP address, an ADDITION_*_ADDRESS message will not be sent to the peers.
- The Gateway does not store the ADDITION_*_ADDRESS information. Any payload with the information from the peer is ignored.
- Retransmission/Dead Peer Detection (DPD) timeout must be configured with a larger value when the MOBIKE feature is enabled.

Standards Compliance

This feature complies with the following standard(s):

- RFC 4555 - IKEv2 Mobility and Multi-homing Protocol (MOBIKE)

Configuring IKEv2 Mobility and Multi-homing Protocol

Enabling IKEv2 Mobility and Multi-homing Protocol

Use the following configuration under the Crypto Template Configuration Mode to enable the MOBIKE feature:

```
config
   context context_name
      crypto template template_name ikev2-dynamic
         ikev2-ikesa mobike [ cookie-challenge ]
         end
```

- Use the **default ikev2-ikesa mobike** command to restore the configuration to its default setting. By default, mobike is disabled.
- If previously configured, use the **no ikev2-kesa mobike** command to remove the configuration.
- Use the **cookie-challenge** keyword to enable the return routability check. The Gateway performs a return routability check when MOBIKE is enabled along with this keyword. This configuration is disabled by default.

Monitoring and Troubleshooting IKEv2 Mobility and Multi-homing Protocol

IKEv2 Mobility and Multi-homing Protocol Show Command(s) and/or Outputs

show crypto ikev2-ikesa security-associations

The following field is available to the output of the **show crypto ikev2-ikesa security-associations** command to indicate if the MOBIKE feature is supported:

```
Mobike Supported         :  Enabled
```

*Table 1: **show crypto ikev2-ikesa security-associations** Command Output Descriptions*

Field	Description
Mobike Supported	Indicates if the MOBIKE feature is supported for this IKEv2 security association.

show crypto statistics ikev2

The following fields are available to the output of the **show crypto statistics ikev2** command in support of this feature:

```
Total IKEv2 Notify Message Receive Statistics:
    MOBIKE Supported:         2   Additional IPv4 Address:     0
    Additional IPv6 Address:  0   No Additional Address:       0
    Update SA Addresses:      2   COOKIE2:                     0
    No NAT Allowed:           0

 Total IKEv2 MOBIKE Statistics:
    MOBIKE Notify Sent:       2   MOBIKE Notify Rcvd:          2
    MOBIKE Ignored:           0   MOBIKE Unexpected NAT Sent:  0
    MOBIKE Unacceptable Address Sent: 0  MOBIKE Cookie2 Rcvd:  0
    MOBIKE Cookie2 Sent:      0  MOBIKE COOKIE2 Mismatch:      0
```

*Table 2: **show crypto statistics ikev2** Command Output Descriptions*

Field	Description
Total IKEv2 Notify Message Receive Statistics:	
MOBIKE Supported	Total number of MOBIKE_SUPPORTED notify payload received.
Additional IPv4 Address	Total number of additional IPv4 addresses received from the peers.
Additional IPv6 Address	Total number of additional IPv6 addresses received from the peers.
No Additional Address	Total number of NO_ADDITIONAL_ADDRESSES notify payload received.
Update SA Addresses	Total number of UPDATE_SA_ADDRESSES notify payload received.
COOKIE2	Total number of COOKIE2 notify payload received.
No NAT Allowed	Total number of NO_NATS_ALLOWED notify payload received.
Total IKEv2 MOBIKE Statistics:	
MOBIKE Notify Sent	Total number of MOBIKE_SUPPORTED notify payload sent from Gateway.
MOBIKE Notify Rcvd	Total number of MOBIKE_SUPPORTED notify payload received and processed successfully.
MOBIKE Ignored	Total number of MOBIKE_SUPPORTED notify payload received, processed and ignored.
MOBIKE Unexpected NAT Sent	Total number of UNEXPECTED_NAT_DETECTED notify payload sent.
MOBIKE Unacceptable Address Sent	Total number of UNACCEPTABLE_ADDRESSES notify payload sent by the Gateway.
MOBIKE Cookie2 Rcvd	Total number of COOKIE2 notify payload received and decoded successfully.
MOBIKE Cookie2 Sent	Total number of COOKIE2 notify payload sent.

Field	Description
MOBIKE COOKIE2 Mismatch	Total number of Cookie2 mismatch occurrences at the Gateway

show crypto template

The following field is available to the output of the **show crypto template** command to indicate if the MOBIKE feature is enabled:

```
IKEv2 Mobike          :  Enabled
```

*Table 3: **show crypto template** Command Output Descriptions*

Field	Description
IKEv2 Mobike	Indicates if the MOBIKE feature is enabled or disabled for this crypto template.

IKEv2 Mobility and Multi-homing Protocol Bulk Statistics

The following bulks statistics included in the System schema support this feature:

Variable	Description	Data Type
ikev2-mobike-sent	**Description**: Total number of MOBIKE_SUPPORTED notify payload sent from Gateway. **Triggers**: Increments when MOBIKE_SUPPORTED notify payload is sent from the Gateway in IKE_AUTH response. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-mobike-recv	**Description**: Total number of MOBIKE_SUPPORTED notify payload received and processed successfully. **Triggers**: Increments when the MOBIKE_SUPPORTED payload received in the IKE_AUTH request is processed. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-mobike-ignored	**Description**: Total number of MOBIKE_SUPPORTED notify payload received, processed and ignored. **Triggers**: Increments when the received MOBIKE_SUPPORTED notify payload is processed and ignored, when it is received in the IKE_AUTH request as MOBIKE is not configured on the Gateway. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32

Variable	Description	Data Type
ikev2-mobike-unexpected-natt-detected-sent	**Description**: Total number of UNEXPECTED_NAT_DETECTED notify payload sent. **Triggers**: **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-mobike-cookie2-rcvd	**Description**: Total number of COOKIE2 notify payload received and decoded successfully. **Triggers**: Increments when UNEXPECTED_NAT_DETECTED is sent in IKEv2 exchange response because NO_NATS_ALLOWED notify payload was received in IKEv2 exchange request and natt is detected. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-mobike-cookie2-sent	**Description**: Total number of COOKIE2 notify payload sent. **Triggers**: Increments when COOKIE2 notify payload is received and decoded successfully. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-mobike-cookie2-mismatch	**Description**: Total number of Cookie2 mismatch occurrences at the Gateway. **Triggers**: Increments when COOKIE2 notify payload is sent from the Gateway. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-mobike-cookie2-match	**Description**: Total number of Cookie2 matched. **Triggers**: Increments when COOKIE2 notify payload is received in IKEv2 exchange response and is different from the Cookie2 sent in IKEv2 exchange request. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32

Variable	Description	Data Type
ikev2-notifrecv-mobikesupp	**Description**: Total number of MOBIKE_SUPPORTED notify payload received. **Triggers**: Increments when COOKIE2 notify payload is received in IKEv2 exchange response and is same as the Cookie2 sent in IKEv2 exchange request. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-notifrecv-updsaaddr	**Description**: Total number of UPDATE_SA_ADDRESSES notify payload received. **Triggers**: Increments when MOBIKE_SUPPORTED notify payload is received in any IKEv2 exchange. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-notifrecv-cookie2	**Description**: Total number of COOKIE2 notify payload received. **Triggers**: Increments when COOKIE2 notify payload is received in any IKEv2 exchange. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32
ikev2-notifrecv-nonatallow	**Description**: Total number of NO_NATS_ALLOWED notify payload received. **Triggers**: Increments when NO_NATS_ALLOWED notify is received in any IKEv2 exchange. **Availability**: Service independent. IPSec Subscriber mode. **Type**: Counter	Int32