IKEv2 Fragmentation

This feature enables IPSec to fragment large messages at IKEv2 as defined in *RFC 7383*.

The following topics are discussed:

Feature Description

Overview

Most Internet Key Exchange (IKEv2) messages are usually small. IP defines a mechanism for fragmentation of oversized UDP messages, but implementations vary in the maximum message size supported. Some NAT and/or Firewall implementations and intermittent routers do not handle IP fragments and these fragmented packets might be dropped. This can cause issues when large IKEv2 messages like digital certificates are transferred over the network.

With this feature, IPSec can fragment large messages at IKEv2 itself and replace them with a series of smaller messages as defined in RFC 7383. The IP datagrams are small enough that fragmentation does not occur at the IP level.

How IKEv2 Fragmentation Works

Fragmenting IKEv2 DL Packets

Only messages that contain an Encrypted payload are subject to IKE fragmentation. For the purpose of construction of IKE Fragment messages, the original (unencrypted) content of the Encrypted payload is split into chunks. The content is treated as a binary blob and is split regardless of the boundaries of inner payloads. Each of the resulting chunks is treated as an original content of the Encrypted Fragment payload, and is encrypted and authenticated. The Encrypted Fragment payload thus contains a chunk of the original content of the Encrypted payload in encrypted form. The Encrypted Fragment payload, if present in a message, will be the last payload in the message.

The maximum fragmentation size is selected based on the value configured through the CLI under the Crypto Template Configuration Mode. For more information, refer *Configuring MTU Size for the IKEv2 Payload*.

Re-assembling IKEv2 Fragmented UL Packets

IPSec receives the encrypted IKEv2 packets and decrypts the encrypted payload. If all fragments are not received, IPSec maintains a timer of 10 seconds, after which the fragments are discarded.

IPSec drops the received fragmented packets during the following scenarios:

- When the received fragment is already present in the buffer.
- When the received fragment exceeds the maximum IKEv2 fragments (255) allowed.
- When each fragment's size exceeds 1932 bytes for IPv4 and 1912 bytes for IPv6.
- When the packet size exceeds 10,000 bytes after re-assembly.

Limitations and Restrictions

This section identifies limitations and restrictions for IKEv2 fragmentation:

- Since IKE Fragment messages are cryptographically protected, SK_a and SK_e must already be calculated. In general, the original message can be fragmented if and only if it contains an encrypted payload. Unprotected payloads cannot be fragmented.
- Among existing IKEv2 extensions, messages of an IKE_SESSION_RESUME exchange, as defined in RFC 5723 cannot be fragmented.
- The Gateway allows fragmenting of IKEv2 packet in downlink, and re-assembling of received IKEv2 packet only if "fragmentation_supported" is negotiated by both peers.
- If the received IKEv2 fragments are greater than 255, the fragments are dropped.

Standards Compliance

This feature complies with the following standards:

- RFC 7383 - Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation
- RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2) (for cryptographic processing)

Configuring IKEv2 Fragmentation

Configuring IKESA Fragmentation (Tx) and Re-assembly (Rx)

Use the following configuration to enable or disable IKESA fragmentation (Tx) and re-assembly (Rx):

```
configure
   context context_name
      crypto template template_name ikev2-dynamic
```

```
        [ no | default ] ikev2-ikesa fragmentation
        end
```

Notes:

- If previously configured, use the **no** keyword to disable IKESA fragmentation and re-assembly support.
- Use the **default** keyword to set the configuration to its default value. By default, IKESA fragmentation and re-assembly is allowed.

Configuring MTU Size for the IKEv2 Payload

Use the following configuration to set the Maximum Transmission Unit (MTU) size for the IKEv2 payload over the IPv4 and/or IPv6 tunnels:

```
configure
   context context_name
      crypto template template_name ikev2-dynamic
         { ip | ipv6 } ikev2-mtu ikev2_mtu_size
         end
```

Notes:

- Use the **default ip ikev2-mtu** or **default ipv6 ikev2-mtu** commands to set the IKEv2 payload to its default value.
- **Default (IPv4):** 1384 bytes
- **Default (IPv6):** 1364 bytes
- *ikev2_mtu_size* (IPv4)must be an integer from 460 through 1932.
- *ikev2_mtu_size* (IPv6)must be an integer from 1144 through 1912.

Monitoring and Troubleshooting IKEv2 Fragmentation

IKEv2 Fragmentation 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 in support of this feature:

```
Fragmentation Supported : Yes
```

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

Field	Description
Fragmentation Supported	Indicates if IKEv2-IKESA fragmentation is supported.

show crypto statistics ikev2

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

```
Control Statistics for Context: <context_name>
  Detailed IKE Statistics:
    Total Fragments In:                    0  Total Fragments Out:                  0
    Total IKE Fragmented Packets In:       0  Total IKE Fragmented Packets out:     0
    Total IKE Fragments Dropped:           0
...
  Total IKEv2 Notify Payload Sent Statistics
    Fragmentation Supported Notify Sent:       0
...
  Total IKEv2 Notify Payload Received Statistics:
    Fragmentation Supported Notify Rcvd:       0
```

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

Field	Description
Detailed IKE Statistics:	
Total Fragments In	Total fragments received.
Total Fragments Out	Total fragments sent.
Total IKE Fragmented Packets In	Total number of IKE fragmented packets received.
Total IKE Fragmented Packets out	Total number of IKE fragmented packets sent.
Total IKE Fragments Dropped	Total number of IKE fragments dropped.
Total IKEv2 Notify Payload Sent Statistics:	
Fragmentation Supported Notify Sent	Total number of IKEv2 Fragmentation Supported notify message sent.
Total IKEv2 Notify Payload Received Statistics:	
Fragmentation Supported Notify Rcvd	Total number of IKEv2 Fragmentation Supported notify message received.

show crypto template

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

```
Map Name: <map_name>
========================================
IKEv2 Fragmentation                  :  Enabled
IKEv2 MTU Size IPv4/IPv6             :  1438/1422
```

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

Field	Description
IKEv2 Fragmentation	Indicates if the configuration for IKEv2 fragmentation is enabled or disabled.
IKEv2 MTU Size IPv4/IPv6	Configured IKEv2 payload MTU size over the IPv4/IPv6 tunnels.

IKEv2 Fragmentation Bulk Statistics

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

Variable	Description	Data Type
ikev2-tx-fragments	**Description:** The total number of fragments transmitted to UE with Internet Key Exchange v2 (IKEv2). **Triggers:** Increments for each fragmented packet transmitted to UE with Internet Key Exchange v2 (IKEv2). **Availability:** System **Type:** Counter	Int32
ikev2-rx-fragments	**Description:** The total number of fragments received from UE with Internet Key Exchange v2 (IKEv2). **Triggers:** Increments for each fragmented packet received from UE with Internet Key Exchange v2 (IKEv2). **Availability:** System **Type:** Counter	Int32
ikev2-tx-fragmented-packet	**Description:** The total number of fragmented packets transmitted to UE with Internet Key Exchange v2 (IKEv2). **Triggers:** Increments if packets are fragmented and transmitted to UE with Internet Key Exchange v2 (IKEv2). **Availability:** System **Type:** Counter	Int32
ikev2-rx-fragmented-packet	**Description:** The total number of fragmented packets received from UE with Internet Key Exchange v2 (IKEv2). **Triggers:** Increments if fragmented packets are received from UE and reassembled with Internet Key Exchange v2 (IKEv2). **Availability:** System **Type:** Counter	Int32

Variable	Description	Data Type
ikev2-rx-fragments-dropped	**Description:** The total number of fragments received from UE dropped with Internet Key Exchange v2 (IKEv2). **Triggers:** Increments for each fragment received from UE dropped with Internet Key Exchange v2 (IKEv2). **Availability:** System **Type:** Counter	Int32