

IKEv2 - Protection Against Distributed Denial of Service

This feature provides security mechanisms for IKEv2 to defend against Distributed Denial-of-Service (DDoS) attacks.

The following topics are discussed:

- Feature Description, on page 1
- How IKEv2 Protection Against DDoS Works, on page 2
- Configuring IKEv2 Protection Against DDoS, on page 3
- Monitoring and Troubleshooting, on page 5

Feature Description

Overview

A distributed denial-of-service (DDoS) attack is caused when multiple malicious systems flood the targeted system with messages in the intention of exhausting the memory of the targeted system. This causes the affected system to run out of sufficient resources to service requests from legitimate peers. Attackers targeting a system can employ any of the following methods:

- Send large amounts of IKE_SA_INIT messages (but no IKE_Auth) for which half-open IKE SA structures are created. This causes the system to utilize resources and run out of memory.
- Send a large amount of junk IKE_Auth packets with correct SPI_i and SPI_r. This causes the system to run out of memory while trying to decrypt the packets.
- Provide an illegitimate URL with a certificate of large size.
- Send continuous SA_INIT packets. This causes the system to run out of memory while trying to generate keys for encrypted packets.
- Send large amounts of rekey requests per second.
- Send large amounts of messages with distinct message IDs. This causes the system to queue all incoming IKE messages, and run out of memory.

This feature provides mechanisms to defend against the DDoS attacks outlined above.

How IKEv2 Protection Against DDoS Works

Architecture

The following prevention mechanisms are available on IPSec against DDoS:

- **Half-open IKE SA timeout** – When an IKE_SA_INIT request is received, a half-open IKE SA timer starts. If an IKE_AUTH message is not received before the timer expires, the half-open IKEv2 IKE SA is cleared. The timer value can be configured using the **ikev2-ikesa ddos half-open-sa-timer** command under the Crypto Template Configuration Mode.
- **Consecutive IKE_AUTH decryption failure detection** – During session creation, if IKE_AUTH decryption fails consecutively for a specified number of times, the IKEv2 IKE SA is cleared. The number of consecutive failure count can be configured using the **ikev2-ikesa ddos decrypt-fail-count** command under the Crypto Template Configuration Mode.

  Alarms will be triggered if decryption fails during post message creation.
- **Certificate validation while downloading** – Downloading large certificates from illegitimate URLs can be avoided by defining the maximum certificate size for the IKE SA. The maximum certificate size can be configured using the **ikev2-ikesa ddos max-cert-size** command under the Crypto Template Configuration Mode.
- **Limit on Child SA re-key per second** – When the specified number of Child SA rekey requests per second is exceeded, TEMPORARY_FAILURE notifications will be sent to the peer to indicate that the peer must slow down their requests. The maximum Child SA re-key request per second can be configured using the **ikev2-ikesa ddos rekey-rate** command under the Crypto Template Configuration Mode.
- **Limit on IKE messages per IKE SA** – When the incoming queued IKE messages per IKE SA exceeds the specified limit, the IKE messages exceeding the limit are dropped. The limit for the IKE messages per IKE SA can be configured using the **ikev2-ikesa ddos message-queue-size** under the Crypto Template Configuration Mode.

For more information on the **ikev2-ikesa ddos** command, refer Configuring IKEv2 Protection Against DDoS, on page 3 of this chapter.

Standards Compliance

This feature complies with the following standards:

- **RFC 7296** – Internet Key Exchange Protocol Version 2 (IKEv2) (for handling DoS attacks)
- IETF reference – "Protecting Internet Key Exchange Protocol version 2 (IKEv2), Implementations from Distributed Denial of Service Attacks"

Configuring IKEv2 Protection Against DDoS

Configuring Half-open SA Timer

Use the following configuration to set the half-open IKE SA timeout duration:

```
config
   context context_name
      crypto template template_name ikev2-dynamic
         ikev2-ikesa ddos half-open-sa-timer half_open_timer_duration
         end
```

Notes:

- *half_open_timer_duration* must be an integer between 1 and 1800.
- **Default**: 60 seconds
- Use the **default ikev2-ikesa ddos half-open-sa-timer** command to restore the configuration to its default value.
- Use the **no ikev2-ikesa ddos half-open-sa-timer** command to disable a previously enabled configuration.

Configuring Decryption Failure Count

Use the following configuration to set the maximum tolerable consecutive IKE_AUTH decryption failure count:

```
config
   context context_name
      crypto template template_name ikev2-dynamic
         ikev2-ikesa ddos decrypt-fail-count failure_count
         end
```

Notes:

- *failure_count* must be an integer between 1 and 100.
- **Default**: 30 times
- Use the **default ikev2-ikesa ddos decrypt-fail-count** keyword to restore the configuration to its default value.
- Use the **no ikev2-ikesa ddos decrypt-fail-count** keyword to disable a previously enabled configuration.

Configuring Re-key Rate

Use the following configuration to set the maximum number of Child SA rekey requests per second:

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

```
ikev2-ikesa ddos rekey-rate rekey_rate_value
end
```

Notes:

- *rekey_rate_value* must be an integer between 1 and 50.
- **Default**: 5
- Use the **default ikev2-ikesa ddos rekey-rate** keyword to restore the configuration to its default value.
- Use the **no ikev2-ikesa ddos rekey-rate** keyword to disable a previously enabled configuration.

Configuring Message Queue Size

Use the following configuration to set the queue size for incoming IKE messages per IKE SA:

```
config
   context context_name
      crypto template template_name ikev2-dynamic
         ikev2-ikesa ddos message-queue-size queue_size
         end
```

Notes:

- *queue_size* must be an integer between 1 and 50.
- **Default**: 20
- Use the **default ikev2-ikesa ddos message-queue-size** keyword to restore the configuration to its default value.
- Use the **no ikev2-ikesa ddos message-queue-size** keyword to disable a previously enabled configuration.

Configuring Maximum Certificate Size

Use the following configuration to set the maximum certificate size for IKE SA:

```
config
   context context_name
      crypto template template_name ikev2-dynamic
         ikev2-ikesa ddos max-cert-size cert_size
         end
```

Notes:

- *cert_size* must be an integer between 512 and 8192.
- **Default**: 2048 bytes
- Use the **default ikev2-ikesa ddos max-cert-size** keyword to restore the configuration to its default value.
- Use the **no ikev2-ikesa ddos max-cert-size** keyword to disable a previously enabled configuration.

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

show crypto ikev2-ikesa security-associations

The following fields are available in the output of the **show crypto ikev2-ikesa security-associations** command in support of this feature:

```
Detailed IKEv2 stats
       0 Request Dropped - Message Queue Size Exceeded
       0 Total IKEv2 IKESA Rekey Requests Temporary Failure Rekey Rate
       0 Total IKEv2 ChildSA Rekey Requests Temporary Failure Rekey Rate
       0 Decryption Fail Count Exceeded
```

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

Field	Description
Detailed IKEv2 stats	
Request Dropped - Message Queue Size Exceeded	Total number of messages dropped due to exceeding the specified queue size.
Total IKEv2 IKESA Rekey Requests Temporary Failure Rekey Rate	Total number of temporary failure messages sent for IKE SA rekey requests due to exceeding the specified rekey rate.
Total IKEv2 ChildSA Rekey Requests Temporary Failure Rekey Rate	Total number of temporary failure messages sent for CHILD SA rekey requests due to exceeding the specified rekey rate.
Decryption Fail Count Exceeded	Total number of messages dropped due to exceeding the specified decryption failure rate.

show crypto statistics ikev2

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

```
Certificate Authentication Statistics:
    Large Certificate Length:             0
Total IKEv2 Timer Expiration Statistics:
    IKE_SA Half Open:                  7 IKE_SA Half Open (No XCHG):           0
Total IKEv2 Child_SA Rekey Statistics:
    IKE_SA Temp Failure Rekey Rate:    0 CHILD_SA Temp Failure Rekey Rate:     0
Total IKEv2 Exchanges Dropped:
    Message Queue Size Exceeded           0
Total IKEv2 Decrypt Failure Statistics:
    Decrypt Fail Count Exceeded           0

IKEv2 DEBUG Statistics:
------------------------------------------------------------------------
       11 tot_ikev2_ikesa_half_open_sa_timer_start
```

```
        0 tot_ikev2_ikesa_half_open_sa_timer_start_ignored
        0 tot_ikev2_ikesa_half_open_sa_timer_stop
------------------------------------------------------------------------
```

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

Field	Description
Certificate Authentication Statistics	
Large Certificate Length	Total IKEv2 certification authentication failures due to large certificate length.
Total IKEv2 Timer Expiration Statistics	
IKE_SA Half Open	The total number of IKESA half open SA timer expirations (valid exchange).
IKE_SA Half Open (No XCHG)	The total number of IKE SA Half Open SA timer expirations (no exchange).
Total IKEv2 Child_SA Rekey Statistics	
IKE_SA Temp Failure Rekey Rate	Total number of temporary failures sent for IKE SA rekey requests due to rekey rate exceeded.
CHILD_SA Temp Failure Rekey Rate	Total number of temporary failures sent for CHILD SA rekey requests due to rekey rate exceeded.
Total IKEv2 Exchanges Dropped	
Message Queue Size Exceeded	The total number of IKEv2 exchanges dropped (message queue size exceeded).
Total IKEv2 Decrypt Failure Statistics	
Decrypt Fail Count Exceeded	Total IKEv2 decryption failures (Fail Count Exceeded).

show crypto template

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

```
IKEv2 IKESA DDOS Mitigation Params:
  IKE SA Half Open Timer: 30
  IKE SA Decrypt Fail Count: 30 [Default]
  IKE SA Message Queue Size: 20 [Default]
  IKE SA Rekey Rate: 5 [Default]
  IKE SA Max Certificate Size: Disabled
```

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

Field	Description
IKEv2 IKESA DDOS Mitigation Params:	

Field	Description
IKE SA Half Open Timer	Configured IKE SA half-open timer duration (in seconds) for the crypto template.
IKESA Decrypt Fail Count	Configured IKE SA decryption failure count for the crypto template.
IKE SA Message Queue Size	Configured IKE SA maximum message queue size for the crypto template.
IKE SA Rekey Rate	Configured IKE SA rekey rate for the crypto template.
IKE SA Max Certificate Size	Configured IKE SA maximum certificate download size (in bytes) for the crypto template.

Bulk Statistics

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

Variable	Description	Data Type
ikev2-exp-half-open-sa-noxchg	**Description:** The total number of IKE SA Half Open SA timer expirations (no exchange). **Triggers:** Increments when a Half Open SA timer expires without any valid exchange. **Availability:** ePDG Service **Type:** Counter	Int32
ikev2-exp-half-open-sa	**Description:** The total number of IKESA half open SA timer expirations (valid exchange). **Triggers:** Increments when a Half Open SA timer expires with a valid exchange. **Availability:** ePDG Service **Type:** Counter	Int32
ikev2-xchg-drop_msg-queuesize-exceeded	**Description:** The total number of IKEv2 exchanges dropped (message queue size exceeded). **Triggers:** Increments when IKEv2 messages get dropped due to message queue size exceeded. **Availability:** ePDG Service **Type:** Counter	Int32

Variable	Description	Data Type
ikev2-decryptfail-count-exceeded	**Description:** Total IKEv2 decryption failures (Fail Count Exceeded). **Triggers:** Increments when IKEv2 decryption failure count exceeds the configured value. **Availability:** ePDG Service **Type:** Counter	Int32
ikev2-ikesa-rekey-rate-temp-failure	**Description:** Total number of temporary failures sent for IKE SA rekey requests due to rekey rate exceeded. **Triggers:** Increments when a temporary failure to IKESA request is sent due to rekey rate exceeded. **Availability:** ePDG Service **Type:** Counter	Int32
ikev2-childsa-rekey-rate-temp-failure	**Description:** Total number of temporary failures sent for CHILD SA rekey requests due to rekey rate exceeded. **Triggers:** Increments when a temporary failure to CHILDSA request is sent due to rekey rate exceeded. **Availability:** ePDG Service **Type:** Counter	Int32
ikev2-cert-auth-fail-large-length	**Description:** Total IKEv2 certification authentication failures due to large certificate length. **Triggers:** Increments when a certificate with a length larger than the configured value is downloaded. **Availability:** ePDG Service **Type:** Counter	Int32

Thresholds

DoS Cookie Challenge

An **IPSecMgr IKEv2 DOS Attack** alarm is generated when the high or low threshold is reached for DOS cookie challenge. The alarm is triggered when the configured DOS cookie challenge reaches the high threshold limit (system is under attack). This alarm is an indication of a security threat. The alarm is cleared when the configured DOS cookie challenge reaches the low threshold limit (system is out of attack).

IKE_Auth Decryption Failure

An **IPSecMgr Decryption Failure** alarm is generated when the high or low threshold is reached for IKE_Auth decryption failure. The alarm is triggered when the configured decryption failure count is reached. The alarm is cleared when the IKEv2 message from the peer is decrypted successfully, or if the session is cleared.

SNMP Traps

The following traps are available to track status and conditions relating to DDoS attack:

- **starIKEv2DOSAttack**: An ipsecmgr facility is under DDOS attack.
- **starIKEv2ClearDOSAttack**: An ipsecmgr facility is out of DDOS attack.

The following traps are available to track status and conditions relating to decryption failure:

- **starIKEv2DecryptionFailThreshold**: The decryption fail count for subsequent IKEV2 messages from a UE exceeds the configured value.
- **starIKEv2ClearDecryptionFailThreshold**: The UE sends a valid IKEv2 packet for which decryption passes.