ePDG DDoS Attack Mitigation

This chapter describes the ePDG DDoS Attack Mitigation feature.

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	**Release**
First introduced.	21.4

Feature Description

ePDG is a network element in EPC Core in the service provider LTE networks that terminates untrusted Wi-Fi. ePDG is reachable via public IP address from UE on UDP port 500/4500. ePDG services UEs from un-secure network making it vulnerable to a host of DDoS attacks. This feature mitigates various types of DDoS attacks.

This section describes high level events/alerts which ePDG mitigates:

UDP/IKE_INIT Decode failure

Attacker can send flood of UDP or IKE_INIT traffic on port 500/4500 from spoofed IP address(es) or compromised hosts (Botnet kind of attacks) from multiple hosts, which in turn will utilize system's CPU and memory, denying services to legitimate users.

No Response for INIT Cookie Challenge or No IKE_AUTH

Attacker can just chose to send valid IKE_INIT requests without sending IKE_AUTH requests for them. If DoS cookie is enabled in the system, and once the half open session hits the threshold. The ePDG will send cookie challenge to peer in order to check if peer is legitimate, but peer is just sending INITs and will not respond to cookie challenge.

All packets till Auth complete

ePDG can face variation of attacks after IKE_INIT transaction is done. Integrity Checksum failure of IKE_AUTH req, Decode Failure after decryption, high rate of junk packets (especially Auth Reqs), or authentication failure if all the subsequent packets are decrypted and decoded successfully.

Attack after Auth Complete

These attacks are result of installing malware, or hacking legitimate user's device. The attacks can be Integrity Check Value (ICV) failure or high data rate of control traffic. ICV failure will utilize CPU resources and high data rate can exhaust the system limit and denying services to legitimate user. High control traffic can include DPD, ike-sa rekey, ipsec-sa rekey, create-child sa req, delete-req etc.

Relationships to Other Features

SR/ICSR Recovery

- SR/Unplanned card migration, monitoring will start from first packet onwards and all data collected before SR/Card migration will be lost. Alarm raised earlier will not be cleared.
- Currently blacklisting of IP address for multiple services of the same IP type is not supported.
- The blacklist IP address configuration is not supported at the boot time. It must be configured once the system is up and running.

How It Works

The ePDG threat detection and mitigation mechanism is implemented to mitigate multiple types of attacks. The following methods describe how to detect a threat from source IP.

UDP Flood / INIT Decode Failure Flood

- A context level failure threshold with upper and lower limit with interval in seconds is configured.
- If the higher threshold is met within the interval, then monitoring will start for each IP address with UDP/INIT packet drops. It will also raise an alarm/SNMP. The alarm will be cleared once the lower threshold is met in any subsequent duration. After the lower threshold is met, IP Address level monitoring will also be stopped.
- Once the upper threshold is met, an alarm/SNMP will be raised with relevant information. The alarm will be cleared for an IP once the lower threshold is met in any subsequent interval.
- Alarm is cleared in next interval once the operator configures the IP address to drop the packets at ipsec demux.

IKE_INIT Flood (no cookie response or no first IKE_AUTH):

- As the attacker can use multiple IP addresses, monitoring INIT storm per source IP address is required.
- A configurable threshold (upper and lower) count per source IP (and/or port) will be used to mark it suspicious and alarm will be raised so that operator can block the IP address.
- Not more than eight IKE_INIT packets should be forwarded to IPSec manager from a single source IP/Port/SPI-I and not more than 8 IKE_INIT with unique SPI_i should be forwarded to IPSec manager from a single Source IP/Port.

Note IPSec cookie configuration and Half-open SA lifetime reduction timeout configuration to mitigate IKE-INIT flood attack are already in place. This new implementation will be an additional way to mitigate the attack.

IKE_AUTH Flood (IKE_AUTH hmac failed or Decode Failed):

- After INIT Request/Response transaction is completed, attacker or device software issue can send flood of Junk IKE_AUTH. Due to which HMAC or decode will fail after decryption, and IMSI will not be available for the scenario.
- For this scenario, process only configured number of HMAC/Decode failures per IKESA. Then delete the session and raise an alarm.

IKE_AUTH Flood (All packets till Auth Complete, after IMSI is available):

- After INIT is completed, attacker can send IKE_AUTH packets on same SPI_i and SPI_r launch high rate of control traffic.
- This can either fail at decryption stage/decode phase
- IPSec manager needs to monitored:

- **Decryption decode fail count**: If threshold crosses the decryption failure, drop the ongoing session and raise an alarm.
- **Decode fail count**: This count only decodes after decryption. This will be counted towards Max IKE request allowed per interval
- **Max IKE request count**: If this request count crosses the threshold, drop ongoing session and raise an alarm

Attack after Auth Complete:

Monitoring Source IP/IMSI SNMP alarm is raised due to block/unblock of IP/IMSI, It will inform all IPSec managers so that once IMSI is available (after authentication) the session can be rejected with appropriate failure notify message.

- Alarm is raised after configured HMAC failure control threshold (upper/lower) fails
- **Control**

Note As part of ePDG DDoS Attack Mitigation Rekey Rate and Half Open Timer along with few other features are implemented in the previous releases. For more details, refer *IKEv2 Protection Against Distributed Denial of Service* of *IPSec Admin Guide*.

- Monitoring is with respect to decryption failure and maximum IKE request allowed per interval
- An alarm is raised once allowed maximum IKE_AUTH phase attempts per interval fails
- Number of IKE/IPSec Rekey per second is limited, notify failure is sent once limit is reached.

Configuring DDoS Attack Mitigation

This section describes the configuration of ePDG DDoS Attack Mitigation.

Configuring IKEv2 Request Rate

Use the following configuration to configure IKEv2 request rate in an interval.

```
configure
   context context_name
      crypto template template_name ikev2-dynamic
        ikev2-ikesa ddos ikev2-req-rate ikev2_req_rate_count [ interval interval
 ]
         { no | default } ikev2-ikesa ddos ikev2-req-rate
         end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association parameters.
- **ddos**: Configures the IKEv2 DDos mitigation parameters.

- **ikev2-req-rate** *ikev2_req_rate_count*: Configures the maximum number of IKEv2 requests allowed per configured interval. *ikev2_req_rate_count* must be an integer from 1 to 3000.

  Default: 10

- **interval** *interval* : Configures the interval for monitoring IKEv2 requests. *interval* must be an integer from 1 to 300.

  Default: 1 second

- **no**: Disables the IKEv2 request count.
- **default**: Sets the default value of the IKEv2 request count.

Configuring INIT Floods

Use the below configuration to configure init flood:

```
configure
   context context_name
      ikev2-ikesa ddos init-flood { source-based | system-based } [
threshold-upper threshold_upper_value  [ threshold-lower threshold_lower_value [
poll-timer-duration poll_timer_duration_value ] ] ]
     { default | no } ikev2-ikesa ddos init-flood { source-based |
system-based }
     end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association Parameters.
- **ddos**: Configures the IKEv2 DDos mitigation parameters.
- **init-flood**: Specifies the IKEv2 DDoS mitigation parameters for INIT Floods.
- **source-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at source IP address level.

  threshold-upper *threshold_upper_value*: Configures upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 100 to 4294967295. Default: 10000.

  threshold-lower *threshold_lower_value*: Configures lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 50 to 4294967294. Default: 5000.

  poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS INIT Floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 30 to 3600. Default: 60 seconds.

- **system-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at system level.

  threshold-upper *threshold_upper_value*: Configures the upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 1000 to 4294967295. Default: 100000.

threshold-lower *threshold_lower_value*: Configures the lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 500 to 4294967294. Default: 50000.

poll-timer-duration *poll_timer_duration_value*: Configures the IKEv2 DDoS INIT floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 60 to 3600. Default: 60 seconds.

- **no**: Removes IKEv2 DDoS mitigation parameters for INIT Floods.
- **default**: Sets the default values for IKEv2 DDoS mitigation parameters for INIT Floods.

Configuring Source Identifiers to Blacklist

Use the following configuration to configure source identifiers to blacklist:

```
configure
   context context_name
      [ no ] ikev2-ikesa ddos blacklist ip-address ipv4_address | ipv6_address
      end
```

Notes:

- **ikev2-ikesa**: Configures the IKEv2 IKE Security Association parameters.
- **ddos**: Configures IKEv2 DDoS mitigation Parameters.
- **blacklist**: Configures the source identifiers to blacklist.
- **ip-address** *ipv4_address* | *ipv6_address*: Configures the source IPv4 or IPv6 address to be blacklisted.
- **no**: Removes the DDoS blacklist configuration.

Configuring UDP Errors

Use the below configuration to configure UDP errors:

```
configure
   context context_name
      ikev2-ikesa ddos udp-error { source-based | system-based } [
threshold-upper threshold_upper_value [ threshold-lower threshold_lower_value [
poll-timer-duration poll_timer_duration_value ] ] ]
     { default | no } ikev2-ikesa ddos udp-error { source-based |
system-based }
     end
```

Notes:

- **ikev2-ikesa**: Configures IKEv2 IKE Security Association Parameters.
- **udp-error**: Specifies IKEv2 DDoS mitigation parameters for UDP errors.
- **source-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for UDP errors applicable at source IP address level.

threshold-upper *threshold_upper_value*: Configures the upper threshold value for error, after which alarm will be raised. *threshold_upper_value* must be an integer from 100 to 4294967295. Default: 10000.

threshold-lower *threshold_lower_value*: Configures the lower threshold value for error, after which alarm will be cleared. *threshold_lower_value* must be an integer from 50 to 4294967294. Default: 5000.

poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS UDP errors timer duration in seconds. *poll_timer_duration_value* must be an integer from 30 to 3600. Default: 60 seconds.

- **system-based threshold-upper** *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

  Configures the IKEv2 DDoS mitigation parameters for UDP errors applicable at system level.

  threshold-upper *threshold_upper_value*: Configures upper threshold value for error, after which alarm will be raised. *threshold_upper_value* must be an integer from 1000 to 4294967295. Default: 100000.

  threshold-lower *threshold_lower_value*: Configures lower threshold value for error, after which alarm will be cleared. *threshold_lower_value* must be an integer from 500 to 4294967294. Default: 50000.

  poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS UDP errors timer duration in seconds. *poll_timer_duration_value* must be an integer from 60 to 3600. Default: 60 seconds.

- **no**: Removes IKEv2 DDoS mitigation parameters for UDP errors.
- **default**: Sets the default values for IKEv2 DDoS mitigation parameters for UDP errors.

Monitoring and Troubleshooting

This section provides information on alarms and thresholds for the DDoS Attack Mitigation feature.

Alarms and Thresholds

The following alarms are added in support of this feature:

- IKEv2DDOSAttackUDPFail
- IKEv2DDOSAttackUDPFailClear
- IKEv2DDOSAttackUDPPeerFail
- IKEv2DDOSAttackUDPPeerFailClear
- IKEv2DDOSAttackINITFlood
- IKEv2DDOSAttackINITFloodClear
- IKEv2DDOSAttackINITPeerFlood
- IKEv2DDOSAttackINITPeerFloodClear
- IKEv2ReqRateThreshold
- IKEv2ClearReqRateThreshold