TDoS Attack Mitigation

The TDoS Attack Mitigation feature enables Cisco Unified Border Element (Cisco UBE) to not respond to Session Initiation Protocol (SIP) requests from IP addresses that are not listed in a trusted IP address list. Cisco UBE validates only out-of-dialog SIP requests against IP addresses in the trusted IP address list. It does not validate in-dialog SIP requests because such requests usually arrive from trusted entities. The TDoS Attack Mitigation feature is supported both on IPv4 and IPv6 networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About TDoS Attack Mitigation

The TDoS Attack Mitigation feature prevents Cisco Unified Border Element (Cisco UBE) from responding to Session Initiation Protocol (SIP) requests arriving from untrusted IP addresses, which leads to an improvement in performance. The SIP stack authenticates the source IP address of an incoming SIP request and blocks the response if the source IP address does not match any IP address in the trusted IP address list. To create a trusted IP address list, you may configure a list of IP addresses or use the IP addresses that have been configured using the **session target** command in dial-peer configuration mode.

Cisco UBE does not respond to REGISTER requests and consumes REGISTER requests if you configure it only for Telephony Denial-of-Service (TDoS) Attack Mitigation and not as a registrar server.

If you configure Cisco UBE as a registrar server for TDoS attack mitigation, it consumes responses for REGISTER requests that do not belong to any application. Cisco UBE does not consume responses to REGISTER requests that belong to a registrar application.

Note A SIP registrar is a server that accepts REGISTER requests and is typically collocated with a proxy or redirect server.

Syslogs are printed on the device console every 60 minutes after Cisco UBE consumes a threshold value of 1000 SIP requests.

How to Configure TDoS Attack Mitigation

Configuring a Trusted IP Address List for Toll-Fraud Prevention

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted list**
5. **ipv4** *ipv4-address* [*network-mask*]
6. **ipv6** *ipv6-address*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters global VoIP configuration mode.

	Command or Action	Purpose
Step 4	**ip address trusted list** **Example:** `Device(conf-voi-serv)# ip address trusted list`	Enters IP address trusted list mode and enables the addition of valid IP addresses.
Step 5	**ipv4** *ipv4-address* [*network-mask*] **Example:** `Device(cfg-iptrust-list)# ipv4 192.0.2.1 255.255.255.0`	Allows you to add up to 100 IPv4 addresses in the IP address trusted list. Duplicate IP addresses are not allowed. • The *network-mask* argument allows you to define a subnet IP address.
Step 6	**ipv6** *ipv6-address* **Example:** `Device(cfg-iptrust-list)# ipv6 2001:DB8:0:ABCD::1/48`	Allows you to add IPv6 addresses to the trusted IP address list.
Step 7	**end** **Example:** `Device(cfg-iptrust-list)# end`	Returns to privileged EXEC mode.

Configuring TDoS Attack Mitigation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted authenticate**
5. **allow-connections** *from-type* **to** *to-type*
6. **sip**
7. **no registrar server**
8. **silent-discard untrusted**
9. **end**
10. **show sip-ua statistics**
11. **clear sip-ua statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**ip address trusted authenticate** **Example:** `Device(conf-voi-serv)# ip address trusted authenticate`	Enables IP address authentication on incoming H.323 or Session Initiation Protocol (SIP) trunk calls for toll fraud prevention support.
Step 5	**allow-connections** *from-type* **to** *to-type* **Example:** `Device(conf-voi-serv)# allow-connections sip to sip`	Allows connections between specific types of endpoints in a Cisco UBE.
Step 6	**sip** **Example:** `Device(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 7	**no registrar server** **Example:** `Device(conf-serv-sip)# no registrar server`	Disables the local SIP registrar.
Step 8	**silent-discard untrusted** **Example:** `Device(conf-serv-sip)# silent-discard untrusted`	Discards SIP requests from untrusted sources on an incoming SIP trunk.
Step 9	**end** **Example:** `Device(conf-serv-sip)# end`	Returns to privileged EXEC mode.
Step 10	**show sip-ua statistics** **Example:** `Device# show sip-ua statistics`	(Optional) Displays response, traffic, and retry SIP statistics.
Step 11	**clear sip-ua statistics** **Example:** `Device# clear sip-ua statistics`	(Optional) Resets the SIP user agent (UA) statistical counters to zero.

Verifying TDoS Attack Mitigation

Sample output for the show sip-ua statistics command

To display response, traffic, and retry Session Initiation Protocol (SIP) statistics, use the **show sip-ua statistics** command in privileged EXEC mode.

```
Device# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
    Success:
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0,
      OkPrack 0/0, OkRegister 0/0
      OkSubscribe 0/0, OkNotify 0/0, OkPublish 0/0
      OkInfo 0/0, OkUpdate 0/0,
      202Accepted 0/0, OkOptions 0/0
    Redirection (Inbound only except for MovedTemp(Inbound/Outbound)) :
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0/0, UseProxy 0,
      AlternateService 0
    Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      ConditionalRequestFailed 0/0,
      ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
      UnsupportedMediaType 0/0, UnsupportedURIScheme 0/0,
      BadExtension 0/0, IntervalTooBrief 0/0,
      TempNotAvailable 0/0, CallLegNonExistent 0/0,
      LoopDetected 0/0, TooManyHops 0/0,
      AddrIncomplete 0/0, Ambiguous 0/0,
      BusyHere 0/0, RequestCancel 0/0,
      NotAcceptableMedia 0/0, BadEvent 0/0,
      SETooSmall 0/0, RequestPending 0/0,
      UnsupportedResourcePriority 0/0,
      Total untrusted Request Consumed 1500,//This counter increments (+1) on reception of
 an untrusted SIP request.//
      Untrusted Request Consumed in last lap 300,//This counter is updated after every 60
minutes.//
      Last Threshold for Untrusted Request Consumed 1000//This counter activates when the
router boots up. Counter value is the number of untrusted requests that are consumed (after
 crossing 1000 SIP requests) in each interval of 60 minutes after the router boots up.//
    Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
    Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0
    Miscellaneous counters:
      RedirectRspMappedToClientErr 0

SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 0/0, Ack 0/0, Bye 0/0,
    Cancel 0/0, Options 0/0,
```

```
    Prack 0/0, Update 0/0,
    Subscribe 0/0, Notify 0/0, Publish 0/0
    Refer 0/0, Info 0/0,
    Register 0/0

Retry Statistics
    Invite 0, Bye 0, Cancel 0, Response 0,
    Prack 0, Reliable1xx 0, Notify 0, Info 0
    Register 0 Subscribe 0 Update 0 Options 0
    Publish 0

SDP application statistics:
 Parses: 0,  Builds 0
 Invalid token order: 0,  Invalid param: 0
 Not SDP desc: 0,  No resource: 0

Last time SIP Statistics were cleared: <never>
```

Configuration Examples for TDoS Attack Mitigation

Example: Trusted IP Address List Configuration

The following example shows how to configure a Trusted IP Address list.

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# ip address trusted list
Device(cfg-iptrust-list)# ipv4 192.0.2.1
Device(cfg-iptrust-list)# ipv6 2001:DB8:0:ABCD::1/48
```

Example: TDoS Attack Mitigation Configuration

The following example shows how to configure TDoS Attack Mitigation.

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# ip address trusted authenticate
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# no registrar server
Device(conf-serv-sip)# silent-discard untrusted
```

Feature Information for TDoS Attack Mitigation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 1: Feature Information for TDoS Mitigation

Feature Name	Release	Feature Information
TDoS Attack Mitigation	15.3(3)M	The TDoS Attack Mitigation feature enables Cisco UBE to not respond to Session Initiation Protocol (SIP) requests from IP addresses that are not listed in a trusted IP address list.
TDoS Attack Mitigation	Cisco IOS XE Release 3.10S	The TDoS Attack Mitigation feature enables Cisco UBE to not respond to Session Initiation Protocol (SIP) requests from IP addresses that are not listed in a trusted IP address list.