CHAPTER 12

DoS Prevention and Dynamic Blacklisting

Denial of Service (DoS) prevention and dynamic blacklisting is used by Cisco Unified Border Element (SP Edition) to block malicious endpoints from attacking the network.

Cisco Unified Border Element (SP Edition) monitors signaling traffic and dynamically detects potential attacks without disrupting the rest of the services that it provides. The attacks can then be blocked internally or externally.

DoS attacks are generally performed on Internet services to deny these services to others. They are usually aimed at the provider of the service, and are either purely malicious vandalism or part of an attempt at extortion.

Blacklisting is the process of matching inbound packets based on parameters, such as source IP addresses, and preventing the packets that match those parameters from being processed.

Dynamic blacklists put in place automatically (subject to a set of configurable constraints) by Cisco Unified Border Element (SP Edition) when it detects an attempt to disrupt traffic flowing through it. Dynamic blacklisting does not require management interference. It can occur within milliseconds of the start of an attack and can change and adapt as the attack changes providing immediate network protection.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html.

For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

Note For Cisco IOS XR Software Release , this feature is supported in the unified model only.

Feature History for DoS Prevention and Dynamic Blacklisting

Release	Modification
Cisco IOS XE Release 2.4	This feature was introduced in Cisco IOS XR along with support for the unified model.
Cisco IOS XE Release 3. 2S	Minor, major, and critical alert traps introduced. The policy-rejection event was renamed as cac-policy-rejection, and the routing-failure event was renamed as rtg-policy-rejection. The na-policy-rejection event was introduced.

Contents

This chapter contains the following sections:

Prerequisites for DoS Prevention and Dynamic Blacklisting

Following are the prerequisites are required for dynamic blacklisting:

- You must already have Cisco Unified Border Element (SP Edition) configured.
- You need to configure blacklisting to override default blacklisting thresholds when the SBE is configured and before you start using Cisco Unified Border Element (SP Edition).

Restrictions for DoS Prevention and Dynamic Blacklisting

The following are restrictions for DoS prevention and dynamic blacklisting:

- Only Session Initiation Protocol (SIP) traffic is analyzed. Attacks over H.323 are not protected. However, an attack over SIP may also result in H.323 traffic being blocked.
- Port specific blacklist configuration is not possible.

Information About DoS Prevention and Dynamic Blacklisting

Cisco Unified Border Element (SP Edition) monitors the following events as "reasons" for initiating DoS detection policies:

- **authentication-failure**—If Cisco Unified Border Element (SP Edition) is locally authenticating the UAs or peers, then any authentication failure will count as one event.
- **bad-address**—This event is generated when an unexpected source sends a packet that reaches Cisco Unified Border Element (SP Edition); the packet will be dropped.
- **rtg-policy-rejection**—This event is generated when traffic fails to find a match in the routing policy. In Cisco IOS XE Release 3.2S, the routing-failure event is renamed as rtg-policy-rejection.
- **endpoint-registration**— This event is generated when an endpoint is registering through Cisco Unified Border Element (SP Edition) and the registration is rejected.
- **corrupt-message**—This event is generated when a signalling message cannot be decoded by the application or contains a protocol exception/violation.

- **cac-policy-rejection**—This is a complex category because it monitors CAC policy failures, that is, a negative result from the CAC policy. This category includes rate, count, and bandwidth limits, and makes no distinction between them. In Cisco IOS XE Release 3.2S, the policy-rejection event is renamed as cac-policy-rejection.
- **spam**—Endpoints may send unwanted or spam calls (sometimes called Spam over Internet Telephony (SPIT)). Spam results from too many unexpected signaling messages. Examples of spam include receipt of a SIP response that does not match an earlier sent request, and receipt of excessive retransmissions of a SIP message.
- **na-policy-rejection**—This event is generated when there are repeated call rejections due to an invalid source number or destination number. This event is considered as a DoS attack.

There are two types of events that would cause blacklisting: low-level and high-level attacks.

- Low-level attacks

  An overwhelming volume of traffic sent at line rate to devices that perform a significant amount of processing per packet.

- High-level attacks

  Attacks on any bottlenecks within the signaling plane or application layers.

Blacklist enablement is defined as 'When an 'E'vent (for example, authentication-failure) that is being monitored, occurs exceeding the 'N'umber of times configured (trigger-size <>) within the 'W'indow (trigger-period <>), then activate the dynamic access control list for a 'T'ime period (timeout <>).

Any given endpoint can have up to three blacklisted events being monitored at a given time on a per-port, per-address, and per-VPN basis. Within the address source type, there is the following order of precedence:

- Limits configured per specific IPv4 address
- Default limits of the parent VRF address space
- Default limits of the global address space (if different from the parent VRF)
- The hard-coded address limits.

The SBC packet filter (SPF) is a new component designed to defend against low-level attacks. The SPF resides with the Media Packet Forwarder (MPF) component on the network processing unit (NPU) and provides low-level DoS prevention for standalone data border element (DBE) and unified SBC deployment scenarios.

A new component is added to the signaling border element (SBE) to detect high-level attacks and create dynamic blacklists based on these attacks. The dynamic blacklist is configured using the command line interface (CLI). It receives events from other SBE components and generates alerts to start or stop the blacklisting of certain messages. Events that might form part of a high-level attack are detected by other SBE components and sent to the SBE Dynamic Blacklisting Component to collects statistics on their rate of occurrence.

Blacklist Alert Traps

From Cisco IOS Release XE 3.2S, the blacklist settings are configured to implement alert traps. Minor, major, and critical traps are set to be triggered at much lower thresholds values. Blacklist alert traps do not cause any loss of service and not only generate a log message when the threshold is exceeded, but also an SNMP trap, if configured. To enable SNMP SBC blacklist traps, use the **snmp-server enable traps sbc blacklist** command.

These traps can be monitored and modified to detect a DoS attack.

Overriding Dynamic Blacklisting Default Thresholds

Dynamic blacklisting is on by default. Default thresholds are set for Trigger Size, Trigger Period, and Blacklisting Period for each reason. A reason may be an Authentication Failure, Bad Address, Routing Failure, Endpoint Registration, Corrupt Message, Spam, Routing Policy Rejection, or Number Analysis Policy Rejection.

We highly recommend you configure blacklisting to override default thresholds for call setup and registration messages at the time the SBE is configured and before you start using Cisco Unified Border Element (SP Edition). Doing this will ensure that your planned call setup rate or registration message rate does not trigger spam blacklist that will impede traffic flow. It is important to configure the call setup or registration messages thresholds to be above the messages or registration messages per second rate for each SIP-based call in order for traffic to flow through properly. The default values for Trigger Size, Trigger Period, and Blacklisting Period are 40 events per second, or 4 events per 100 milliseconds. This means that traffic over 40 packets per second would trigger blacklisting.

For the following SIP-based call flow, this example describes how to calculate a suitable trigger size threshold for call setup messages per second:

```
SIP-based call (caller) has:
Send INVITE
Receive 100 Trying
Receive 180 Ringing
Receive 200 OK to confirm Session Establishment
Send ACK to complete Session Establishment
Send BYE
Receive 200 OK
===================================
SIP-based call (callee) has:
Send INVITE
Send 100 Trying
Send 180 Ringing
Send 200 OK to confirm Session Establishment
Receive ACK to complete Session Establishment
Receive BYE
Send 200 OK
============================================
```

There are 14 messages or packets for each SIP-based call. If you have a call setup rate of up to 20 calls per second (CPS), then 14 messages x 20 CPS = 280 messages per second. Therefore for a call setup rate of up to 20 CPS, you would configure a trigger size threshold of at least 280 messages per second.

In the following configuration example, you have raised the trigger size to 280 messages or packets per second:

```
blacklist global
 reason spam
  trigger-size 280
  trigger-period 1 seconds
```

Similar to calculating call set up messages per second, the following example describes how to calculate a suitable trigger size threshold for registration messages:

There is one message per registration per second for each SIP-based call. If you have 20 registrations per second, then 1 messages x 20 registrations = 20 messages per second. Therefore for a registration rate of up to 20 registrations per second, you would configure a trigger size threshold of at least 20 messages per second.

Although Dynamic Blacklisting is on by default, you can turn it off by setting the timeout for every reason to zero. However, note that when timeout is set to zero for any unit value, such as milliseconds or seconds, the unit value returned in a **show run** command displays as "day." You can use the **show sbc sbe blacklist configured-limits** command to display the default trigger-size, trigger-period and timeout and configured limits. See ?$paranum>Examples of Using the show Commands with Blacklisting? section on page 12-11 for an example of this command.

Dynamic Blacklisting Behavior

The following is a description of dynamic blacklisting behavior:

- A global rate limit is applied to ensure that the overall load across all sources and destinations does not exceed the CPU capacity (the default limiter 8000 pps/1000 Mbps).
- The hard-coded initial settings for each event type on each IP address are configured by default to hold 4 events for 100 milliseconds. If the configured values are exceeded, the IP address is blacklisted for 10 minutes.
- If you have an explicitly configured limit for a single IP address or port, any trigger and blocking time values defined in that configuration will override the default. Table 12-1 displays where the parameters of the event limits at each scope for a given message can be configured. The limits are different if the message source is on a global address space or VPN.
- Media packets must match a valid entry in the flow table or they are dropped.

Table 12-1 Priority of Event Limit Parameters

Scope of Event Limit	Event Limit Parameter Sources (Highest Priority First)	
	Global Address Space	VPN
Port	1. Explicit limit for this port 2. Default for this IP address	1. Explicit limit for this port 2. Default for this IP address
Address	1. Explicit limit for this address 2. Default for global IP addresses 3. Hard-coded initial settings	1. Explicit limit for this address 2. Default for addresses on this VPN 3. Default for global IP addresses 4. Hard-coded initial settings
VPN	Explicit limit for the global address space.	1. Explicit limit for this VPN 2. Limit set for the global address space

- Valid media packets must not exceed bandwidth limits established in call signaling. Non-conferment packets are dropped.
- Signaling packets are rate-limited by the source port in an attempt to halt forceful packet floods early (the default limiter is 1000 pps/100 mpbs).
- Signaling packets that are not destined to a valid local port are dropped.
- Signaling packets are rate-limited by destination port (the default limiter is 4000 pps/500 Mbps).
- Limits can be configured for specific events from the following source(s): a VPN ID, an IP address, or a port at a specific IP address.

- Default limits on event rates may be defined for all source IP addresses on a VPN, and for all ports on a given IP address. The default limits on each IP address are automatically set at the start of the day, but their parameters can be reconfigured. By default, no event limits are configured for ports.

  Cisco Unified Border Element (SP Edition) monitors events per IP address by default. You can also configure Cisco Unified Border Element (SP Edition) to monitor an entire VPN or a particular port. If any limit in a VPN is then exceeded, the entire VPN is blacklisted. If a limit for a port is exceeded, the port and its IP address are blacklisted.
- Packets are classified as either signaling or media according to the port from where they are sent:
  - Ports below 10,000 are signaling.
  - Ports above 10,000 are media.
- When only a global address space blacklist is defined (no VRF specific blacklist), this will be used to blacklist addresses in all configured VRFs.
- VRF based blacklist limits will override any per source or address-default limits already set. You cannot use per IP address scope to override behavior in VRF space.
- Cisco Unified Border Element (SP Edition) generates an SNMP trap when a blacklist is activated.

How to Configure Dynamic Blacklisting

You can configure dynamic blacklisting as explained in the following sections:

- Configuring Blacklist Parameters for an IP Address, Port, or VPN, page 12-6
- Configuring an End to Blacklisting, page 12-9

Configuring Blacklist Parameters for an IP Address, Port, or VPN

To configure the event limits for a specific source, use the following commands.

Note You must configure blacklisting to override the default blacklisting thresholds when the SBE is configured, and before you start using Cisco Unified Border Element (SP Edition).

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **blacklist ipv4** *addr*
5. **description** *text*
6. **reason** *event*
7. **trigger-size** *number*
8. **trigger-period** *time*
9. **critical-alert-size** *number-of-events*
10. **major-alert-size** *number-of-events*

11. **minor-alert-size** *number-of-events*
12. **timeout** *timeframe*
13. **end**
14. **show sbc** *service-name* **sbe blacklist configured-limits**
15. **show sbc** *service-name* **sbe blacklist** *source*
16. **show sbc** *service-name* **sbe blacklist current-blacklisting**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`configure terminal`**
	Example:
	`Router# configure`
		Enables global configuration mode.

Step 2	**`sbc`** *`service-name`*
	Example:
	`Router(config)# sbc mysbc`
		Creates the SBC service on Cisco Unified Border Element (SP Edition) and enters the SBC configuration mode.

Step 3	**`sbe`**
	Example:
	`Router(config)# sbe`
		Enters the SBE entity mode within an SBC service.

Step 4	**`blacklist ipv4`** *`addr`*
	Example:
	`Router(config)# blacklist ipv4 25.25.25.5`
		Enters the blacklist submode for configuring the event limits for a given source.
		The **no** form of this command changes the event limits that have been configured to default values.
		Note Event limit parameters that are not configured in this submode are configured with the default, as follows:
		– port—port-default value for its address.
		– IP address—address-default value for the VPN.
		– VPN—value for the global address space.
		– global address space—no limit.

Step 5	**`description`** *`text`*
	Example:
	`Router(config-sbc-sbe-blacklist)# description NAT of XYZ Corp`
		Adds a description for the source and its event limits using a readable text string format.
		The **no** form of this command removes the description.
		This description is displayed when the **show** command is used for this source.

	Command or Action	Purpose
Step 6	**reason** *event* **Example:** `Router(config-sbc-sbe-blacklist)# reason authentication-failure`	Enters the reason submode for configuring a limit for a specific event type on the source. The **no** form of this command returns the event limit to its default values. An event includes: • authentication-failure—Requests that fail authentication. • bad-address—Packets from unexpected addresses. • rtg-policy-rejection—Requests that fail to be routed by SBC. • endpoint-registration—All endpoint registrations. • cac-policy-rejection—Requests that are rejected by the CAC policy. • corrupt-message—Signaling packets that are too corrupt to be parsed by the relevant protocol. • na-policy-rejection—Requests that are rejected by the configured number analysis policy.
Step 7	**trigger-size** *number* **Example:** `Router(config-sbc-sbe-blacklist-reason# trigger-size 5`	Defines the number of events from the specified source that are allowed before the blacklisting is triggered and all packets are blocked from the source. Range can be 0 to 65535,
Step 8	**trigger-period** *time* **Example:** `Router(config-sbc-sbe-blacklist-reason)# trigger-period 20 milliseconds`	Defines the period of time that events are considered. *time* is expressed as *number unit* where *number* is an integer and *unit* is one of: milliseconds, seconds, minutes, hours, or days. Default period of time is between 10 milliseconds and 23 days.
Step 9	**timeout** *time* **Example:** `Router(config-sbc-sbe-blacklist-reason)# timeout 180 seconds`	Defines the length of time when packets from the source are blocked if the configured limit is exceeded. *time* can have the following values: • 0 = the source is not blacklisted • never = the blacklisting is permanent • *number unit* where *number* is an integer and *unit* is seconds, minutes, hours, or days Default period of time is less than 23 days.
Step 10	**critical-alert-size** *number-of-events* **Example:** `Router(config-sbc-sbe-blacklist-reason)# critical-alert-size 655`	Defines the number of specified events that must occur before the critical alert is triggered. *number-of-events* can have any value ranging from 1 to 65535.

	Command or Action	Purpose
Step 11	**major-alert-size** *number-of-events* **Example:** Router(config-sbc-sbe-blacklist-reason)# major-alert-size 300	Defines the number of specified events that must occur before the major alert is triggered. *number-of-events* can have any value ranging from 1 to 65535.
Step 12	**minor-alert-size** *number-of-events* **Example:** Router(config-sbc-sbe-blacklist-reason)# minor-alert-size 20	Defines the number of specified events that must occur before the minor alert is triggered. *number-of-events* can have any value ranging from 1 to 65535.
Step 13	**end** **Example:** Router(config-sbc-sbe-blacklist-reason)# **end**	Exits the reason mode and enters Privileged EXEC mode.
Step 14	**show sbc** *service-name* **sbe blacklist configured-limits** **Example:** Router# show sbc mysbc sbe blacklist global configured-limits	Displays detailed information about the explicitly configured limits. Any values not explicitly defined for each source are displayed in brackets.
Step 15	**show sbc** *service-name* **sbe blacklist** *source* **Example:** Router# show sbc mysbc sbe blacklist vpn3 ipv4 172.19.12.12	List the limits that are currently in place for a specific source (in this example, VPN). This includes any defaults or explicitly configured limits. It also includes any defaults of a smaller scope that are configured at this address. Any values that are not explicitly configured are bracketed (these are the values that are inherited from other defaults).
Step 16	**show sbc** *service-name* **sbe blacklist current-blacklisting** **Example:** Router# show sbc mysbc sbe blacklist current-blacklisting	Lists the limits that are causing the source(s) to be blacklisted.

Configuring an End to Blacklisting

Use the following command to remove the source from the blacklist:

- **clear sbc** *service-name* **sbe blacklist** *source*

For the *service-name* parameter, enter the name of the SBC.

For the *source* parameter enter the name of the blacklist.

Examples of Configuring, Removing, and Displaying Dynamic Blacklisting

This section provides a sample configuration and output for dynamic blacklisting, removing a source from being blacklisted, and also displaying configured limits.

Example of Configuring Dynamic Blacklisting

This blacklist is configured for global address space with one authentication failure from all possible address sources to be captured within a 100 milliseconds window. The ACL created (blacklist) should never timeout.

```
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist)# address-default
Router(config-sbc-sbe-blacklist-addr-default)# reason authentication-failure
Router(config-sbc-sbe-blacklist-addr-default)# timeout never
Router(config-sbc-sbe-blacklist-addr-default)# trigger-size 1
Router(config-sbc-sbe-blacklist-addr-default)# trigger-period 100 milliseconds
```

This blacklist is configured for global address space, five packets from unexpected source within a one minute window. The ACL is to time out in 24 hours.

```
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist)# ipv4 10.5.1.21
Router(config-sbc-sbe-blacklist-ipv4)# reason bad-address
Router(config-sbc-sbe-blacklist-ipv4)# timeout 1 days
Router(config-sbc-sbe-blacklist-ipv4-reason)# trigger-size 5
Router(config-sbc-sbe-blacklist-ipv4-reason)# trigger-period 1 minutes
```

Example of Removing a Source from the Blacklist

The following example shows the syntax for removing blacklist from Cisco Unified Border Element (SP Edition):

```
Router# clear sbc mysbc sbe blacklist blacklist
Router#
```

Example of Displaying All the Configured Limits

The following example shows the configured limits for various types of blacklisting:

```
Router# show sbc uut105-1 sbe blacklist configured-limits

SBC Service "uut105-1"

Blacklist Defaults
====================
Reason            Trigger     Trigger  Blacklisting    Minor    Major  Critical
                     Size      Period        Period    Alert    Alert     Alert
Auth-failure          (4)    (100 ms)     (10 mins)  not set  not set   not set
Bad-address           (4)    (100 ms)     (10 mins)  not set  not set   not set
RTG-policy-rejection  (4)    (100 ms)     (10 mins)  not set  not set   not set
Endpoint-registration (4)    (100 ms)     (10 mins)  not set  not set   not set
CAC-policy-rejection  (4)    (100 ms)     (10 mins)  not set  not set   not set
Corrupt-message       (4)    (100 ms)     (10 mins)  not set  not set   not set
```

```
Spam                 (30)    (100 ms)     (10 mins)  not set  not set   not set
NA-policy-rejection   (4)    (100 ms)     (10 mins)  not set  not set   not set

--------------------------------------------------------------

VRF:  172.18.53.56
====================
Reason            Trigger     Trigger  Blacklisting    Minor    Major  Critical
                     Size      Period        Period    Alert    Alert     Alert
NA-policy-rejection   (4)    (100 ms)     (10 mins)        2  not set   not set

--------------------------------------------------------------
Router#
```

Examples of Using the show Commands with Blacklisting

The following example shows the command required to list the limits that are currently in place for a specific source (in this example, VPN). This includes any defaults or explicitly configured limits. It also includes any defaults of a smaller scope that are configured at this address. Any values that are not explicitly configured are bracketed (these are the values that are inherited from other defaults).

```
Router# show sbc mysbc sbe blacklist vpn3 ipv4 172.19.12.12

SBC Service "mySbc" SBE dynamic blacklist vpn3 172.19.12.12

vpn3 172.19.12.12
=================
Reason          Trigger          Trigger      Blacklisting
                   Size           Period            Period
------          -------          -------      ------------
Authentication     (20)            10 ms          (1 hour)
Bad address        (20)            10 ms          (1 hour)
Routing            (20)            10 ms          (1 hour)
Registration        (5)           100 ms        (10 hours)
Policy             (20)            10 ms           (1 day)
Corrupt              40            10 ms          (1 hour)

Default for ports of vpn3 172.19.12.12
======================================
Reason          Trigger          Trigger      Blacklisting
                   Size           Period            Period
------          -------          -------      ------------
Authentication       20            1 sec            1 hour
Bad address          20            1 sec            1 hour
Routing              20            1 sec            1 hour
Registration          5           30 sec          10 hours
Policy               20            1 sec             1 day
Corrupt              20           100 ms            1 hour
```

The following example shows the command required to list the limits that are causing the source(s) to be blacklisted:

```
Router# show sbc mysbc sbe blacklist current-blacklisting

SBC Service "mySbc" SBE dynamic blacklist current members

Global addresses
================
Source           Source   Blacklist       Time
Address          Port     Reason          Remaining
-------          ------   ---------       ---------
```

```
125.125.111.123  All      Authentication  15 mins
125.125.111.253  UDP 85   Registration    10 secs
144.12.12.4      TCP 80   Corruption      Never ends

VRF: vpn3
=========
Source           Source   Blacklist       Time
Address          Port     Reason          Remaining
-------          ------   ---------       ---------
132.15.1.2       TCP 285  Registration    112 secs
172.23.22.2      All      Policy          10 hours
```

The following example shows the configured limits:

```
Router# show sbc MySBC sbe blacklist configured-limits

SBC Service "MySBC"

Blacklist Defaults
====================
Reason            Trigger     Trigger  Blacklisting    Minor    Major  Critical
                     Size      Period        Period    Alert    Alert     Alert
Auth-failure          (4)    (100 ms)     (10 mins)  not set  not set   not set
Bad-address           (4)    (100 ms)     (10 mins)  not set  not set   not set
RTG-policy-rejection  (4)    (100 ms)     (10 mins)  not set  not set   not set
Endpoint-registration (4)    (100 ms)     (10 mins)  not set  not set   not set
CAC-policy-rejection  (4)    (100 ms)     (10 mins)  not set  not set   not set
Corrupt-message       (4)    (100 ms)     (10 mins)  not set  not set   not set
Spam                 (30)    (100 ms)     (10 mins)  not set  not set   not set
NA-policy-rejection   (4)    (100 ms)     (10 mins)  not set  not set   not set

--------------------------------------------------------------

VRF:  172.18.53.56
====================
Reason            Trigger     Trigger  Blacklisting    Minor    Major  Critical
                     Size      Period        Period    Alert    Alert     Alert
NA-policy-rejection   (4)    (100 ms)     (10 mins)        2  not set   not set

--------------------------------------------------------------
```

Note Watch out for the default configurations already in effect. Only the applied configurations are modified.

This example shows current blacklisting:

```
Router# show sbc MySBC sbe blacklist current-blacklisting

SBC Service "MySBC" SBE dynamic blacklist current members

Global addresses
================
Source           Source   Blacklist       Time
Address          Port     Reason          Remaining
-------          ------   ---------       ---------
10.5.1.31All      Authentication  Forever
```