



# DoS Prevention and Dynamic Blacklisting

---

Denial of Service (DoS) prevention and dynamic blacklisting is used by the SBC to block malicious endpoints from attacking the network.

The SBC must monitor signaling traffic and dynamically detect 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 the SBC 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.

## Feature History for Restricting Codecs

Release	Modification
Release 3.4.1	This feature was introduced on the Cisco XR 12000 Series Router.
Release 3.5.0	No modification.
Release 3.6.0	No modification.

## Contents

This module contains the following sections:

- [Prerequisites for DoS Prevention and Dynamic Blacklisting, page SBC-252](#)
- [Restrictions for DoS Prevention and Dynamic Blacklisting, page SBC-252](#)
- [Information About DoS Prevention and Dynamic Blacklisting, page SBC-253](#)
- [How to Configure Dynamic Blacklisting, page SBC-254](#)
- [Examples of Configuring, Removing, and Displaying Dynamic Blacklisting, page SBC-257](#)
- [Additional References, page SBC-260](#)

## Prerequisites for DoS Prevention and Dynamic Blacklisting

The following prerequisites are required for dynamic blacklisting:

- You must be in a user group associated with a task group that includes the proper task IDs for SBC commands being used. For detailed information about user groups and task IDs, see the defined task ID required per command in the *Cisco IOS XR Session Border Controller Command Reference*.
- You must install and activate the package installation envelope (PIE) for the SBC software.  
For detailed information about PIE installation, refer to the *Upgrading and Managing Cisco IOS XR Software* module in the *Cisco IOS XR Getting Started Guide*.
- The SBC must already be created. See the procedures described in the [SBC Configuration Prerequisites](#) section.

## Restrictions for DoS Prevention and Dynamic Blacklisting

Review the following restrictions for dynamic blacklisting:

- Only SIP traffic is analyzed in this release. Attacks over H.323 are not protected. However, an attack over SIP may also result in H.323 traffic being blocked.
- Packets are classified as either signaling or media according to the port where they are sent:
  - Ports below 10,000 are signaling
  - Ports above 10,000 are media
- 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 mpbs).
- The hard-coded initial settings for each event type on each IP address are configured 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 15](#) 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.

**Table 15** Priority of Event Limit Parameters

Scope of Event Limit	Event Limit Parameter Sources (Highest Priority First)	
	Global Address Space	VPN
Port	<ol style="list-style-type: none"> <li>Explicit limit for this port</li> <li>Default for this IP address</li> </ol>	<ol style="list-style-type: none"> <li>Explicit limit for this port</li> <li>Default for this IP address</li> </ol>

**Table 15** *Priority of Event Limit Parameters (continued)*

Scope of Event Limit	Event Limit Parameter Sources (Highest Priority First)	
	Global Address Space	VPN
Address	<ol style="list-style-type: none"> <li>1. Explicit limit for this address</li> <li>2. Default for global IP addresses</li> <li>3. Hard-coded initial settings</li> </ol>	<ol style="list-style-type: none"> <li>1. Explicit limit for this address</li> <li>2. Default for addresses on this VPN</li> <li>3. Default for global IP addresses</li> <li>4. Hard-coded initial settings</li> </ol>
VPN	Explicit limit for the global address space.	<ol style="list-style-type: none"> <li>1. Explicit limit for this VPN</li> <li>2. Limit set for the global address space</li> </ol>

## Information About DoS Prevention and Dynamic Blacklisting

There are two types of events that might indicate behavior that would cause blacklisting: low- 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.

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

A new component is added to the SBE to detect high-level attacks and create dynamic blacklists based on these attacks. The dynamic blacklist is configured using the 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 collect statistics on their rate of occurrence.

Dynamic blacklisting limitations:

- Media packets must match a valid entry in the flow table or they are dropped.
- 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 mpbs).
- 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 day, but their parameters can be reconfigured. By default, no event limits are configured for ports.

The SBC monitors events per IP address by default. You can also configure the SBC 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.

The SBC applies a default event limit to each limit source, but you can change them.

## 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 SBC-254](#)
- [Configuring an End to Blacklisting, page SBC-257](#)

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

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

#### SUMMARY STEPS

1. **configure**
2. **sbc *service-name* sbe blacklist *source***
3. **description *text***
4. **reason *event***
5. **trigger-size *number***
6. **trigger-period *time***
7. **timeout *timeframe***
8. **exit**
9. **exit**
10. **commit**
11. **show services sbc *service-name* sbe blacklist configured-limits**
12. **show services sbc *service-name* sbe blacklist *source***
13. **show services sbc *service-name* sbe blacklist current-blacklisting**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure</b>  <b>Example:</b> RP/0/0/CPU0:router# <b>configure</b>	Enables global configuration mode.
Step 2	<b>sbc service-name sbe blacklist source</b>  <b>Example:</b> RP/0/0/CPU0:router(config)# <b>sbc mysbc sbe blacklist ipv4 25.25.25.5</b>	<p>Enters the submode for configuring the event limits for a given source.</p> <p>Use the <i>service-name</i> argument to define the name of the service.</p> <p>The <b>no</b> version of this command returns the limits to the default values.</p> <p><b>Note</b> Any 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</p>
Step 3	<b>description text</b>  <b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe-blacklist)# <b>description NAT of XYZ Corp</b>	<p>Adds a description for source and its event limits using a readable text string format.</p> <p>The <b>no</b> form of this command removes the description.</p> <p>This description is displayed when the <b>show</b> command is used for this source.</p>
Step 4	<b>reason event</b>  <b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe-blacklist)# <b>reason authentication-failure</b>	<p>Enters a submode for configuring a limit for a specific event type on the source.</p> <p>The <b>no</b> form of this command returns the event limit to its default values.</p> <p>An event includes:</p> <ul style="list-style-type: none"> <li>• authentication-failure (requests that fail to be authenticated)</li> <li>• bad-address (packets from unexpected addresses)</li> <li>• routing-failure (requests that fail to be routed by SBC)</li> <li>• endpoint-registration (all endpoint registrations)</li> <li>• policy-rejection (requests that are rejected by configured policy)</li> <li>• corrupt-message (signaling packets that are too corrupt to be parsed by the relevant protocol)</li> </ul>
Step 5	<b>trigger-size number</b>  <b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe-blacklist-reason)# <b>trigger-size 5</b>	<p>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.</p> <p>Range can be 0 to 65535,</p>

	Command or Action	Purpose
Step 6	<p><b>trigger-period</b> <i>time</i></p> <p><b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe-blacklist-reason)# <b>trigger-period 20 milliseconds</b></p>	<p>Defines the period of time that events are considered.</p> <p><i>time</i> is expressed as <i>&lt;number&gt; &lt;unit&gt;</i> where <i>number</i> is an integer and <i>unit</i> is one of: milliseconds, seconds, minutes, hours, or days.</p> <p>Default period of time is between 10 milliseconds and 23 days.</p>
Step 7	<p><b>timeout</b> <i>time</i></p> <p><b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe-blacklist-reason)# <b>timeout 180 seconds</b></p>	<p>Defines the length of time when packets from the source are blocked if the configured limit is exceeded.</p> <p><i>time</i> can have the following values:</p> <ul style="list-style-type: none"> <li>• 0 = the source is not blacklisted</li> <li>• never = the blacklisting is permanent</li> <li>• <i>&lt;number&gt; &lt;unit&gt;</i> where <i>number</i> is an integer and <i>unit</i> is seconds, minutes, hours, or days (select one)</li> </ul> <p>Default period of time is less than 23 days.</p>
Step 8	<p><b>exit</b></p> <p><b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe-blacklist-reason)# <b>exit</b></p>	<p>Exits the reason mode to the blacklist mode.</p>
Step 9	<p><b>exit</b></p> <p><b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe-blacklist)# <b>exit</b></p>	<p>Exits the blacklist mode to the SBE mode.</p>
Step 10	<p><b>commit</b></p> <p><b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe)# <b>commit</b></p>	<p>Saves configuration changes. Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</p>
Step 11	<p><b>show services sbc</b> <i>service-name</i> <b>sbe blacklist configured-limits</b></p> <p><b>Example:</b> RP/0/0/CPU0:router(config-sbc-sbe)# <b>show sbc mysbc sbe blacklist configured-limits</b></p>	<p>Displays detailed information about the explicitly configured limits.</p> <p>Any values not explicitly defined for each source are displayed in brackets.</p>

	Command or Action	Purpose
Step 12	<pre>show services sbc service-name sbe blacklist source</pre> <p><b>Example:</b>  RP/0/0/CPU0:router(config-sbc-sbe)# <b>show sbc mysbc sbe blacklist vpn3 ipv4 172.19.12.12</b></p>	<p>List the limits that are currently in place for a specific source (in this example, VPN). This includes any defaults or explicitly configured limits.</p> <p>It also includes any defaults of a smaller scope that are configured at this address.</p> <p>Any values that are not explicitly configured are bracketed (these are the values that are inherited from other defaults).</p>
Step 13	<pre>show services sbc service-name sbe blacklist current-blacklisting</pre> <p><b>Example:</b>  RP/0/0/CPU0:router(config-sbc-sbe)# <b>show services sbc mysbc sbe blacklist current-blacklisting</b></p>	<p>Lists the limits that are causing the source(s) to be blacklisted.</p>

## Configuring an End to Blacklisting

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

```
clear services 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

The following example shows the commands required to configure a new dynamic blacklist limit on the rate of authentication failure events allowed from the IP address 25.25.25.5.

```
configure
  sbc mysbc
  sbe
  blacklist ipv4 25.25.25.5
  description NAT of XYZ Corp
  reason authentication-failure
  trigger-size 5
  trigger-period 20 milliseconds
  timeout 180 seconds
  exit
exit
commit
```

## Example of Removing a Source from the Blacklist

The following example shows the syntax for removing blacklist from the SBC:

```
RP/0/0/CPU0:PE7_C12406#clear services sbc mysbc sbe blacklist blacklist
RP/0/0/CPU0:PE7_C12406#
```

## Example of Displaying All Configured Limits

The following example shows the command required to list the explicitly configured limits. Any values that are not explicitly defined for each source are in brackets.

```
configure
  show sbc mysbc sbe blacklist configured-limits

SBC Service "mySbc" SBE dynamic blacklist configured limits

Default for all addresses
=====
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

Default for addresses on vpn3
=====
Reason          Trigger          Trigger          Blacklisting
              Size            Period            Period
-----
Authentication    20              1 sec            1 day
Bad address       20              1 sec            1 day
Routing           20              1 sec            1 day
Registration       5               30 sec           1 day
Policy            20              1 sec            1 day
Corrupt           50              100 ms           12 hours

112.234.23.2
=====
Reason          Trigger          Trigger          Blacklisting
              Size            Period            Period
-----
Authentication    2000            (1 sec)          (1 hour)
Bad address       2000            (1 sec)          (1 hour)
Routing           2000            (1 sec)          (1 hour)
Registration       500             (30 sec)         (10 hours)
Policy            2000            (1 sec)          (1 day)
Corrupt           2000            (100 ms)         (1 hour)

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           40          10 ms        (1 hour)

```

```

Default for ports of vpn3 172.19.12.12
=====

```

Reason	Trigger Size	Trigger Period	Blacklisting 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

## Example of Displaying Configured Limits of a Source

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).

```

configure
  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

```

## Example of Displaying the Limits Causing Blacklisting

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

```

configure
  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

```

## Additional References

The following sections provide references related to DoS prevention and dynamic blacklisting.

## Related Documents

Related Topic	Document Title
Cisco IOS XR master command reference	Cisco IOS XR Master Commands List
Cisco IOS XR SBC interface configuration commands	<i>Cisco IOS XR Session Border Controller Command Reference</i>
Initial system bootup and configuration information for a router using the Cisco IOS XR Software	<i>Cisco IOS XR Getting Started Guide</i>
Cisco IOS XR command modes	<i>Cisco IOS XR Command Mode Reference</i>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support from existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

■ Additional References