

DoS Prevention and Dynamic Blacklisting

Denial of Service (DoS) prevention and dynamic blacklisting is used by the Session Border Controller (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.



Note

For ACE SBC Release 3.0.00, this feature is supported in the unified model only.

Feature History for Restricting Codecs

Release	Modification
ACE SBC Release 3.0.00	This feature was introduced on the Cisco 7600 series router along with support for the SBC unified model.

Contents

This module contains the following sections:

- [Prerequisites for DoS Prevention and Dynamic Blacklisting, page 31-2](#)
- [Restrictions for DoS Prevention and Dynamic Blacklisting, page 31-2](#)
- [Information About DoS Prevention and Dynamic Blacklisting, page 31-3](#)
- [How to Configure Dynamic Blacklisting, page 31-4](#)
- [Examples of Configuring, Removing, and Displaying Dynamic Blacklisting, page 31-7](#)

Prerequisites for DoS Prevention and Dynamic Blacklisting

The following prerequisites are required for dynamic blacklisting:

- On the Application Control Engine Module (ACE), you must be an Admin user to enter SBC commands. For more information, see the *Application Control Engine Module Administration Guide* at http://www.cisco.com/en/US/products/hw/modules/ps2706/products_configuration_guide_book09186a00806838f4.html.
- The SBC must already be created. See the procedures described in the [ACE Configuration Prerequisites for the SBC](#) section.

Restrictions for DoS Prevention and Dynamic Blacklisting

Review the following restrictions for dynamic blacklisting:

- Only Session Initiation Protocol (SIP) traffic is analyzed in ACE SBC Release 3.0.00. 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 Mbps).
- 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 31-1](#) 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.
- 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 <>).
- The following events can be monitored as reasons for DOS detection policies:
 - **authentication-failure**—If the SBC 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 the SBC; the packet will be dropped.
 - **routing-failure**—This event is generated when traffic fails to find a match in routing policy.
 - **endpoint-registration**— This event is generated when an end point is registering through the SBC 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.

- **policy-rejection**—This is a complex category as it essentially monitors for CAC policy failures (that is, a negative result from CAC policy). This category therefore includes rate, count, and bandwidth limits and makes no distinction between them.
- 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.
- 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.
- When a blacklist created dynamic ACL is active, all sessions matching the scope are impacted, including the ones that are active.
- Dynamic ACLs remain active until the expiration of ‘T’ or clearing of the blacklist configuration.
- Port specific blacklist configuration is not possible.
- The SBC does generate an SNMP trap when a blacklist is activated.

Table 31-1 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"> 1. Explicit limit for this port 2. Default for this IP address 	<ol style="list-style-type: none"> 1. Explicit limit for this port 2. Default for this IP address
Address	<ol style="list-style-type: none"> 1. Explicit limit for this address 2. Default for global IP addresses 3. Hard-coded initial settings 	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Explicit limit for this VPN 2. Limit set for the global address space

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 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 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 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 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 31-4](#)
- [Configuring an End to Blacklisting, page 31-7](#)

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. **show services sbc** *service-name* **sbe blacklist** **configured-limits**
11. **show services sbc** *service-name* **sbe blacklist** *source*
12. **show services sbc** *service-name* **sbe blacklist** **current-blacklisting**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: host1/Admin# configure	Enables global configuration mode.
Step 2	sbc <i>service-name</i> sbe blacklist <i>source</i> Example: host1/Admin(config)# sbc mysbc sbe blacklist ipv4 25.25.25.5	Enters the submode for configuring the event limits for a given source. Use the <i>service-name</i> argument to define the name of the service. The no form of this command returns the limits to the default values. Note 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
Step 3	description <i>text</i> Example: host1/Admin(config-sbc-sbe-blacklist)# description NAT of XYZ Corp	Adds a description for 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 4	<p>reason <i>event</i></p> <p>Example: <pre>host1/Admin(config-sbc-sbe-blacklist)# reason authentication-failure</pre></p>	<p>Enters a submode for configuring a limit for a specific event type on the source.</p> <p>The no form of this command returns the event limit to its default values.</p> <p>An event includes:</p> <ul style="list-style-type: none"> • authentication-failure (requests that fail to be authenticated) • bad-address (packets from unexpected addresses) • routing-failure (requests that fail to be routed by SBC) • endpoint-registration (all endpoint registrations) • policy-rejection (requests that are rejected by configured policy) • corrupt-message (signaling packets that are too corrupt to be parsed by the relevant protocol)
Step 5	<p>trigger-size <i>number</i></p> <p>Example: <pre>host1/Admin(config-sbc-sbe-blacklist-reason# trigger-size 5</pre></p>	<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>
Step 6	<p>trigger-period <i>time</i></p> <p>Example: <pre>host1/Admin(config-sbc-sbe-blacklist-reason)# trigger-period 20 milliseconds</pre></p>	<p>Defines the period of time that events are considered.</p> <p><i>time</i> is expressed as <i>number unit</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>timeout <i>time</i></p> <p>Example: <pre>host1/Admin(config-sbc-sbe-blacklist-reason)# timeout 180 seconds</pre></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"> • 0 = the source is not blacklisted • never = the blacklisting is permanent • <i>number unit</i> where <i>number</i> is an integer and <i>unit</i> is seconds, minutes, hours, or days <p>Default period of time is less than 23 days.</p>
Step 8	<p>exit</p> <p>Example: <pre>host1/Admin(config-sbc-sbe-blacklist-reason)# exit</pre></p>	<p>Exits the reason mode to the blacklist mode.</p>
Step 9	<p>exit</p> <p>Example: <pre>host1/Admin(config-sbc-sbe-blacklist)# exit</pre></p>	<p>Exits the blacklist mode to the SBE mode.</p>

	Command or Action	Purpose
Step 10	<pre>show services sbc <i>service-name</i> sbe blacklist configured-limits</pre> <p>Example: host1/Admin(config-sbc-sbe)# show sbc mysbc sbe blacklist configured-limits </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>
Step 11	<pre>show services sbc <i>service-name</i> sbe blacklist source</pre> <p>Example: host1/Admin(config-sbc-sbe)# show services sbc mysbc sbe blacklist vpn3 ipv4 172.19.12.12 </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 12	<pre>show services sbc <i>service-name</i> sbe blacklist current-blacklisting</pre> <p>Example: host1/Admin(config-sbc-sbe)# show services sbc mysbc sbe blacklist current-blacklisting </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

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

```
host1/Admin(config-sbc-sbe)# blacklist
host1/Admin(config-sbc-sbe-blacklist)# address-default
host1/Admin(config-sbc-sbe-blacklist-addr-default)# reason authentication-failure
host1/Admin(config-sbc-sbe-blacklist-addr-default)# timeout never
host1/Admin(config-sbc-sbe-blacklist-addr-default)# trigger-size 1
```

```
host1/Admin(config-sbc-sbe-blacklist-addr-default)# trigger-period 100 milliseconds
```

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

```
host1/Admin(config-sbc-sbe-blacklist)# ipv4 10.5.1.21
host1/Admin(config-sbc-sbe-blacklist-ipv4)# reason bad-address
host1/Admin(config-sbc-sbe-blacklist-ipv4)# timeout 1 days
host1/Admin(config-sbc-sbe-blacklist-ipv4-reason)# trigger-size 5
host1/Admin(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 the SBC:

```
host1/Admin# clear services sbc mysbc sbe blacklist blacklist
host1/Admin#
```

Example of Displaying All Configured Limits

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

```
ACE-105-UUT1-1/Admin# show services sbc uut105-1 sbe blacklist configured-limits
SBC Service ''uut105-1''
```

```
Global
=====
Reason Trigger Trigger Blacklisting
Size Period Period
-----
Authentication 30 30 secs 30 secs
Bad Address (0) (0 days) (0 days)
Routing (0) (0 days) (0 days)
Registration (0) (0 days) (0 days)
Policy (0) (0 days) (0 days)
Corrupt (0) (0 days) (0 days)

vpn1
=====
Reason Trigger Trigger Blacklisting
Size Period Period
-----
Authentication (30) (30 secs) (30 secs)
Bad Address (0) (0 days) (0 days)
Routing (0) (0 days) (0 days)
Registration 50 50 secs 50 secs
Policy (0) (0 days) (0 days)
Corrupt (0) (0 days) (0 days)

Default for all addresses
=====
Reason Trigger Trigger Blacklisting
Size Period Period
-----
Authentication (4) (100 ms) (10 mins)
Bad Address (4) (100 ms) (10 mins)
Routing (4) (100 ms) (10 mins)
Registration (4) (100 ms) (10 mins)
Policy (4) (100 ms) (10 mins)
```

```

Corrupt 40 40 secs 40 secs

Admin 1.1.1.1
=====
Reason Trigger Trigger Blacklisting
Size Period Period
-----
Authentication (4) (100 ms) (10 mins)
Bad Address (4) (100 ms) (10 mins)
Routing 10 20 secs 20 secs
Registration (4) (100 ms) (10 mins)
Policy (4) (100 ms) (10 mins)
Corrupt (40) (40 secs) (40 secs)
ACE-105-UUT1-1/Admin#

```

Examples of Using 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).

```

host1/Admin# 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:

```

host1/Admin# 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 Address	Source Port	Blacklist Reason	Time Remaining
132.15.1.2	TCP 285	Registration	112 secs
172.23.22.2	All	Policy	10 hours

This example shows the configured limits:

```
host1/Admin# show services sbc MySBC sbe blacklist configured-limits
SBC Service "MySBC"
```

```
Global
```

```
=====
```

Reason	Trigger Size	Trigger Period	Blacklisting Period
Authentication	(0)	(0 days)	(0 days)
Bad Address	(0)	(0 days)	(0 days)
Routing	(0)	(0 days)	(0 days)
Registration	(0)	(0 days)	(0 days)
Policy	(0)	(0 days)	(0 days)
Corrupt	(0)	(0 days)	(0 days)

```
Default for all addresses
```

```
=====
```

Reason	Trigger Size	Trigger Period	Blacklisting Period
Authentication	1	100 ms	Forever
Bad Address	(4)	(100 ms)	(10 mins)
Routing	(4)	(100 ms)	(10 mins)
Registration	(4)	(100 ms)	(10 mins)
Policy	(4)	(100 ms)	(10 mins)
Corrupt	(4)	(100 ms)	(10 mins)

```
Admin 10.5.1.21
```

```
=====
```

Reason	Trigger Size	Trigger Period	Blacklisting Period
Authentication	(1)	(100 ms)	(Forever)
Bad Address	5	1 mins	1 days
Routing	(4)	(100 ms)	(10 mins)
Registration	(4)	(100 ms)	(10 mins)
Policy	(4)	(100 ms)	(10 mins)
Corrupt	(4)	(100 ms)	(10 mins)



Note

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

This example shows current blacklisting.

```
host1/Admin# show services 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
```

