ERICSSON

Configuring Malicious Traffic Detection and Monitoring

SYSTEM ADMINISTRATOR GUIDE

87/1543-CRA 119 1170/1-V1 Uen K

Contents

1 Overview

The SmartEdge router can detect, count, and log malicious traffic, as well as raise alarms when the count exceeds a certain threshold. This document describes the SmartEdge malicious traffic detection and monitoring feature.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

Included in this document is the following information:

- Overview of malicious traffic handling in the SmartEdge router
- List of malicious traffic types that can be detected and monitored
- Overview of malicious traffic counters, alarms, and logging
- Configuration of malicious traffic detection and monitoring
- Output display examples of show malicious traffic commands
- Configuration examples

2 Malicious Traffic Detection

Malicious traffic detection is addressed in the SmartEdge router through the packet processing ASIC (PPA) using a combination of implicit and configured Layer 3 (L3) and Layer 4 (L4) security checks. This section describes these security checks.

2.1 Restrictions

This section highlights the restrictions of the SmartEdge router malicious traffic detection and monitoring feature:

- Only supported on PPA2 and PPA3 cards.
- Reverse Path Forwarding (RPF) checking for IPv6 traffic at the interface level is not supported.

2.2 Implicit Security Checks

The SmartEdge router performs implicit security checks to detect and drop malicious traffic. To determine which implicit checks are performed, see the Type of Security Check column in Table 1. This table provides information about the reason for dropping a packet (or the security check performed on the packet), whether the security check is implicit or configured, which set of packets were checked, and the drop counter category of malicious traffic the packet falls in.

2.3 Configured Security Checks

The SmartEdge router can perform security checks to detect and drop malicious traffic based on these types of configurations:

Note: Generally, Reverse Path Forwarding (RPF), IP source-address validation (SAV), and ingress filtering all refer to the same functionality.

- **RPF checks**—For IPv4 traffic, you can enable RPF checks on a per-interface basis. Both strict and loose modes are supported. Use the **`ip verify unicast source`** command in the interface configuration mode to perform an RPF check to verify the source IP address on all incoming unicast packets at the specified interface. If the packet passes the RPF check, the packet is forwarded as normal; however, if the router does not find a reverse path for the packet, the packet is dropped. The SmartEdge router counts packets dropped due to failed RPF checks.

Note: RPF checks can optionally be enabled only for traffic that is permitted by ACL rules.

- **IP SAV**—For IPv4 and IPv6 subscriber traffic, you can enable IP SAV, which denies all IP packets from address sources that are not reachable through a subscriber's associated circuit. For IPv6 traffic, use the **`ipv6 source-validation`** command in subscriber configuration mode to enable IP SAV. If the packet passes the IP SAV check, it is forwarded; if the source address is not reachable through the subscriber's associated circuit, the packet is dropped. The SmartEdge router counts packets dropped due to failed IP SAV checks.

  Note: If you have enabled the **`ip verify unicast source`** command in interface configuration mode for IPv4 traffic, you do not need enable the **`ip source-validation`** command in subscriber configuration mode.

- **Packet Filter checks**—You can perform IPv4 and IPv6 packet filtering by configuring IP Access Control Lists (ACLs). ACLs can be applied on an interface, and packets received or sent over the interface are subjected to the rules specified in the ACL. ACLs applied at the context level are called administrative ACLs and only packets sent to the kernel are subjected to this type of ACL.

  The format and function of ACLs are the same regardless of whether they are applied to kernel bound packets or traffic sent or received over interfaces.

  ACL rules can either permit or deny a packet based on the following match criteria:

  – IP header fields—Source address, Destination Address, Protocol, DSCP, ToS, Total Length

  – TCP—Port, Flags

  – UDP—Port

  – ICMP—Type, Code

  – IGMP—Type

  – Fragments

  – IP-options

  Note: IP-options and packet-total-length match criteria are not supported in IPv6 ACLs.

3 Malicious Traffic Counters

If malicious-traffic counting is enabled, the SmartEdge router maintains counters for packets dropped due to implicit and configured checks for malicious traffic listed in Table 1. Context-level drop counters are maintained. Border Gateway Function (BGF) realm-level counters are aggregated at the context level and labeled as "Other" within the output of the **`show malicious-traffic counters`** command.

The SmartEdge router maintains a per-context malicious-traffic counter block containing a number of drop counters. When a packet is dropped, the router increments the appropriate circuit-level, context-level or realm-level drop counter and increments the per-context malicious-traffic counter (if malicious-traffic counting is enabled).

Note: The removal or deletion of circuits or realms does not change the value of the malicious-traffic counters.

Malicious traffic drop counters are grouped by category, and each category is maintained on a per-context basis. The following are the supported categories:

- Reassembly—represents packets dropped because of packet reassembly failures
- Filtered—represents packets dropped because of IP filter ACL
- Malformed-IP—represents packets dropped because of an invalid IP header
- Malformed-Layer4—represents packets dropped because of an invalid L4 header
- Spoofed—represents packets dropped because of RPF or IP SAV failures or because the destination address of the packet resolved to a null route
- Other—represents malicious-traffic drops not counted against the previously listed categories.

Note: Currently, the Other category only includes the aggregate of all the realm-specific drop counters in a given context.

The SmartEdge router collects the counters and determines the cumulative per-context category counters.

Table 1 provides information about the reason for dropping a packet (or the security check performed on the packet), whether the security check is implicit or configured, which set of packets were checked, the drop counter category of malicious traffic the packet falls in, and whether the security check is associated with IPv4, IPv6, or both.

Table 1 Malicious Traffic Drop Reason, Security Check Type, Drop Counter Category

Security Check/Drop Reason	Type of Security Check	Security Checks Performed for Which Packets?	Drop Counter Category	Applicable to IPv4, IPv6, or Both?
IP version other than IPv4 or IPv6	Implicit	all packets	Malformed-IP	Both
Invalid IP header length	Implicit	all packets	Malformed-IP	Both
Invalid IP total length (1)(2)	Implicit	all packets	Malformed-IP	Both
Invalid payload length (3)	Implicit	all packets	Malformed-IP	IPv6
Invalid IP checksum	Implicit	all packets	Malformed-IP	IPv4
Invalid ICMP checksum (4)	Implicit	locally destined packets only	Malformed-Layer4	Both
Invalid UDP length (5)	Implicit	locally destined packets only	Malformed-Layer4	Both
IP Options (6)	Configured	all packets	Malformed-IP	Both
IP filter ACL drops	Configured	all packets	Filtered	Both
RPF failure	Configured	all packets	Spoofed	IPv4
IP SAV failure	Configured	all packets associated with subscriber circuit	Spoofed	Both
Null route	Configured	all packets	Spoofed	Both
Reassembly failures	Implicit	locally destined packets only	Reassembly	IPv4
BGF realm drops	Implicit	forwarded media-plane packets only	Other	Both

(1) IPv4: total length larger than the packet length or IP header length larger than the total length
(2) IPv6: packets with invalid packet length (entire L3 packet length)
(3) IPv6: value of length (payload plus extension header length) in the IPv6 header length field is greater than entire packet length
(4) Dropping ICMP packets with invalid checksum only for those ICMP packets that require the PPA itself to respond. Other locally destined ICMP packets are sent to the kernel, and the kernel validates the checksum.
(5) For example, UDP length that is not equal to that derived from the IP header total length.
(6) For example, dropping packets containing IP options other than Record-Route and Router-Alert.

Table 2 lists the various malicious traffic attack types that can be detected and monitored based on an implicit security check or configured security check using RPF, ACLs, or IP SAVs . Note that this is not a comprehensive list of the types of malicious attacks that the SmartEdge router can protect a network against.

Table 2 Malicious Traffic Attack Types

Attack Type	**Implicit or Configured Security Check**
Short IP header	Implicit
Malformed IP header	Implicit
Unknown protocols	Implicit (BGF Media Plane only), ACL
Invalid IP checksum	Implicit
IP Fragmentation attacks	ACL, Robust local reassembly mechanism
IP Option attacks	Implicit, ACL (using match criteria) to drop packets with any options.
UDP short header	Implicit
Invalid TCP flag combinations	Implicit (SYN+FIN disallowed for realm), ACL (using match criteria)
ICMP attacks	ACL
TCP short header attack	Implicit
TCP packet oversized	Implicit (maximum L4 packet size is configurable for BGF media plane)
Answering TCP packets from a multicast address	ACL
UDP DoS with same source as destination IP address	RPF, ACL
Spoofing attacks	IP SAV, RPF

Multiple drop reasons may get counted against a single circuit-level counter. There is only one counter for packets with invalid IP header length and total length. Similarly, there is only a single circuit-level counter for all packets dropped on account of ACL rules. Thus a breakdown of the drop reasons for the “Filtered” category is not provided.

Packets dropped in the kernel based on administrative ACL rules are not counted in the malicious traffic drop counters.

Malicious-traffic counters reset to 0 after you reload a PPA card. However, the SmartEdge router retains the previous total of malicious-traffic counters before the reload. If malicious-traffic counting is disabled after the reload, the counters are reset to zero.

For more information about ACLs, see *Configuring ACLs*.

4 Malicious Traffic Alarms

A single context-wide alarm against the aggregate of all the drop malicious traffic category counters is supported. There are two alarms:

- High—raised when the delta between the previous and current drop counters in the context exceed the configured high threshold and a high alarm has not already been raised before. (Successive high alarms are not raised.) This alarm indicates the router is under malicious attack.
- Low—raised when the delta between the previous and current drop counters in the context fall below the configured low threshold and a high alarm was previously raised. This alarm indicates that the router is no longer under attack.

Note: Alarms for malicious traffic are raised only at the end of the alarm interval. Thus an alarm interval set for example at one hour is raised until the hour has elapsed even if the alarm criteria is met within 10 minutes of the interval. It is highly recommended that you do not specify a high value for the alarm interval.

Alarms are associated with enabled malicious-traffic counters, and the alarm period begins when counting is enabled for a context. The alarm period is global and applies to all contexts. To enable an alarm for a specific context, use the **`alarms`** command in the malicious-traffic context configuration mode. The default and minimum alarm interval is 60 seconds. The first alarm period for a context may be smaller than the actual configured interval for the given context. You can use the **`show malicious traffic counters`** command to display the remaining time for the alarm expiry.

When a given alarm period ends, the SmartEdge router generates an alarm based on configured thresholds and sends an event log message with a debug logging level of alert (for alert and more severe events) when a malicious traffic alarm is triggered.

Note: In the event of a restart or system switchover, the SmartEdge router sends a low alarm notification if it finds that the high alarm had been raised prior to the restart or switchover.

4.1 Restrictions

If the Statistics daemon does not receive a report on time because of one of the following events, the counters from the delayed report are not counted towards the alarm thresholds for that period:

- PPAs reload

- Statistics daemon restarts
- SNMP daemon restarts
- XCRP switchover

And as a result, an alarm may not be generated.

5 Malicious Traffic Logging

The SmartEdge router supports malicious traffic logging, which is disabled by default. You can configure the router to log dropped packets due to the various implicit and configured security checks mentioned in Table 1. You can also enable logging for a specified category of malicious traffic within a given context. The malicious traffic log messages are provided in a binary or a text format with a log level of informational.

The SmartEdge router supports the storage of traffic logs on local files and syslog servers. For local files, the default file format is binary with the additional option to save in a text file format. Of these two file formats, the binary file format is recommended for better performance. Syslog server logs are only available in a text format. The traffic logs can be tagged with a syslog facility value different from that used for event logs. This allows the syslog servers to store the logs in different files. Logs are always maintained in the in-memory circular buffer regardless of the file or syslog configuration.

To view packet logs stored in the in-memory buffer or in a specified file (binary or text format), use the **`show malicious-traffic log file`** command. To clear packet logs stored in the in-memory buffer or in a specified file (binary or text format), use the **`clear malicious-traffic log file`** command. If a file is specified, all versions of the file are cleared and then logging to these files resumes again.

Note: When using either the **`show malicious-traffic log file`** or the **`clear malicious-traffic log file`** command from a non-local context, only files configured for that context can be viewed or cleared.

Malicious traffic logging is rate-limited. The logging rate and burst parameters are globally configurable. You can specify the maximum rate in packets per second (pps) at which the packets can be received and the maximum number of packets that can be received during a short burst. The specified rate and burst values are distributed evenly across all of the active PPA2 and PPA3 cards. The actual rate limit per active card is obtained by dividing the configured rate limit by the total number of active PPA2 and PPA3 cards. The same calculation applies to obtaining the actual burst limit for each active PPA2 or PPA3 card.

Keep the following in mind about malicious traffic logging:

- You can configure up to four malicious traffic log files for each context, each with a unique file name.
- Malicious traffic logs are not printed on the console.
- If malicious traffic logging is enabled in the local context using either a local file and syslog server, malicious packets from all the other contexts are logged to the file or server in the local context.

- During a Logging process restart (after a crash recovery) or a router switchover, malicious traffic is not logged.

Like the other system event log files, you can use up to seven files to store the malicious traffic logs. Each file can be maximum of 1 MB and older log files are saved as compressed files in a gzip file format. When 80% of the total malicious-traffic log file capacity (7 MB) is used, the SmartEdge router generates an alert message indicating that the file is near full capacity. Another alert message is generated after 100% capacity is reached and logging to these files ceases. Logging resumes only after these files are cleared using the **`clear malicious-traffic log file`** command.

Note: Before clearing the files, it is recommended you transfer the files to another location using the **`copy`** command with the File Transfer Protocol (FTP). See Page 17 for more information.

The in-memory buffer logging continues even after file capacity is reached. Each 1 MB log file can store approximately 8K of IPv4 and IPv6 packets in a binary format and approximately 4K in a text format. The actual number may vary depending on the size and contents of the packet.

6 Configuration and Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see *Command List*, which provides links to the documentation of all SmartEdge router commands.

6.1 Summary of Configuration

The following is a summary of the steps to take to configure malicious traffic detection and monitoring:

1. Optional. For IPv4 traffic, enable RPF on a per-interface basis to detect malicious traffic. See Table 3.
2. Optional. For IPv6 traffic, enable IP source-address validation to detect malicious traffic. See Table 4.
3. Configure IP Access Control Lists for packet filtering to detect malicious traffic. To configure IPv4 ACLs, see Table 3. To configure IPv6 ACLs, see Table 4.
4. Optional. Configure malicious traffic parameters at the global level. See Table 5.
5. Configure malicious traffic parameters at the context level. See Table 6.
6. Perform monitoring and troubleshooting of malicious traffic. See Table 7.

The following is a summary of the steps to take to configure malicious traffic detection and monitoring:

6.2 Configure Malicious Traffic Detection

To detect IPv4 malicious traffic, configure RPFs and ACLs. Perform the tasks described in Table 3. For more information on ACLs, see *Configuring ACLs*.

Table 3 Configure Malicious Traffic Detection for IPv4 Traffic Using RPF and ACLs

Step	Task	Root Command	Notes
1.	Optional. Configure to perform an RPF check to verify the source IP address on all incoming unicast packets at the specified interface.	*ip verify unicast source*	interface configuration mode
2. Configure IPv4 ACLs.			

Table 3 Configure Malicious Traffic Detection for IPv4 Traffic Using RPF and ACLs

Step	Task	Root Command	Notes
2a.	Create an ACL and enter access control list configuration mode to add options and rules.	*ip access-list*	Enter this command in context configuration mode.
2b.	Optional. Associate a description with an IP ACL.	*description (ACL)*	
2c.	Optional. Create ACL statements using either or both of the following tasks:		
	Create an ACL statement using **`permit`** conditions.	*permit* or *seq*	To explicitly set its order in the list, use the **`seq permit`** construct for each statement.
	Create an ACL statement using **`deny`** conditions.	*deny* or *seq*	To explicitly set its order in the list, use the **`seq deny`** construct for each statement.
3. Apply an IPv4 ACL.			
3a.	Apply an IP ACL to an interface or to a subscriber record, named profile, or default profile.	*ip access-group* (interfaces and subscribers)	Enter this command in either interface or subscriber configuration mode.
3b.	Apply an IP ACL to a context.	*admin-access-group*	Enter this command in context configuration mode.

To detect IPv6 malicious traffic, configure IP SAVs and ACLs. Perform the tasks described in Table 4.

Table 4 Configure Malicious Traffic Detection for IPv6 Traffic Using IP SAVs and ACLs

Step	Task	Root Command	Notes
1.	Optional. Configure to enable IP source-address validation, which denies all IP packets from address sources that are not reachable through a subscriber's associated circuit.	*ipv6 source-validation*	subscriber configuration mode
2. Configure IPv6 ACLs.			

Table 4 Configure Malicious Traffic Detection for IPv6 Traffic Using IP SAVs and ACLs

Step	Task	Root Command	Notes
2a.	Create an ACL and enter access control list configuration mode to add options and rules.	*ipv6 access-list*	Enter this command in context configuration mode. On PPA2 card, a maximum of 100 rules can be added to each ACL. On PPA3 card, a maximum of 8192 rules can be added to each ACL.
2b.	Optional. Associate a description with an IP ACL.	*description (ACL)*	
2c.	Optional. Create ACL statements using either or both of the following tasks:		
	Create an ACL statement using **`permit`** conditions.	*permit* or *seq*	To explicitly set its order in the list, use the **`seq permit`** construct for each statement.
	Create an ACL statement using **`deny`** conditions.	*deny* or *seq*	To explicitly set its order in the list, use the **`seq deny`** construct for each statement.
3. Apply an IPv6 ACL.			
3a.	Apply an IP ACL to an interface or to a subscriber record, named profile, or default profile.	*ipv6 access-group*	Enter this command in interface mode.
3b.	Apply an IP ACL to a context.	*ipv6 admin-access-group*	Enter this command in context configuration mode.

6.3 Configure Malicious Traffic Monitoring at Global Level

By default, if you enable malicious traffic monitoring at the context level, the default global parameters for malicious traffic monitoring is applied for the global level. Therefore, it is not required that you configure malicious traffic monitoring parameters in global configuration mode. However, you are still required to enable the Simple Network Management Protocol (SNMP) server provided Step 6 in Table 5. To customize the default global values for malicious traffic monitoring, perform all of the tasks in Table 5. Enter all commands in malicious-traffic configuration mode, unless otherwise noted.

For information about the malicious traffic-related commands listed in Table 5 , see Reference [1].

Table 5 Configure Malicious Traffic Monitoring at Global Level

Step	Task	Root Command	Notes
1.	Optional. Configure malicious traffic parameters and enter malicious-traffic configuration mode.	*malicious-traffic*	global configuration mode.
2.	Optional. Specify the rate and burst limits for malicious traffic log events.	*logging rate-limit*	
3.	Optional. Configure alarm parameters for malicious traffic and enter malicious-traffic alarms configuration mode.	*alarms*	
4.	Optional. Specify the high and low threshold values (in packets) for malicious traffic alarms.	*threshold (malicious traffic)*	malicious-traffic alarms configuration mode
5.	Optional. Configure the amount of time between the reporting of malicious-traffic counters.	*interval (malicious traffic)*	malicious-traffic alarms configuration mode
6.	Enable the Simple Network Management Protocol (SNMP) server to which malicious traffic alarms are sent.	*snmp server*	global configuration mode

6.4 Configure Malicious Traffic Monitoring at Context Level

To monitor malicious traffic in a given context, you must first enable the monitoring in the context. To enable malicious traffic monitoring in a context, perform the tasks described in Table 6; enter all commands in context configuration mode, unless otherwise noted.

For information about the malicious traffic-related commands listed in Table 6, see Reference [1].

Table 6 Configure Malicious Traffic Monitoring at Context Level

Step	Task	Root Command	Notes
1.	Enable logging of a specified category of malicious traffic.	*logging malicious-traffic category*	

Table 6 Configure Malicious Traffic Monitoring at Context Level

Step	Task	Root Command	Notes
2.	Optional. Enable logging of malicious traffic messages to a binary or text file.	*logging malicious-traffic file [text]*	
3.	Optional. Enable the logging of malicious traffic messages to a remote syslog server that is reachable within the context.	*logging malicious-traffic syslog*	
4.	Enter malicious-traffic context configuration mode to configure malicious traffic parameters for the given context.	*malicious-traffic*	
5.	Enable the collection of statistics for malicious traffic.	*counters (malicious traffic)*	Malicious-traffic context configuration mode
6.	Enable an alarm to be generated when the counters reach a certain threshold for malicious traffic	*alarms*	Malicious-traffic context configuration mode

6.5 Monitoring and Troubleshooting Malicious Traffic

6.5.1 Operations Tasks

To monitor and troubleshoot malicious traffic, perform the operations tasks described in Table 7. Enter the **`show`** commands in any mode.

Table 7 Operations Tasks

Task	Root Command	Notes
Display contents of malicious-traffic in-memory buffer log.	*show malicious-traffic log*	
Display packet logs stored in the in-memory buffer or in a specified file (which may be in either binary or text format).	*show malicious-traffic log file <filename>*	

Table 7 Operations Tasks

Task	Root Command	Notes
Display malicious-traffic counters.	*show malicious-traffic counters*	In addition to the counters, this command displays the alarm state.
Clear the malicious traffic log files. This clears all of the seven files.	*clear malicious-traffic log file*	Before clearing the files, it is highly recommended to transfer the files to another location using the **copy** command using File Transfer Protocol (FTP). This procedure assumes that a system exists that is reachable by the SmartEdge router to service these requests. For more information, see the **copy** command.
Clear the malicious traffic in-memory buffer log files.	*clear malicious-traffic log*	
Display malicious-traffic counters at the circuit level.	*show circuit counters detail*	You can use this command to view the drop counters corresponding to many of the drop reasons listed in Table 1. You can use the information from the command output to identify the circuits on which the malicious traffic is received and the type of malicious traffic detected.

6.5.2 Show Malicious Traffic Output Display Examples

The following example displays output from the **show malicious log** command for IPv4 traffic. In the first line of the output, the context ID `[0001]` and the circuit handle `3/8:1023:63/1/1/20510]` are in bold. This data indicates from which context and circuit the malicious traffic was detected and dropped.

```
[local]Redback#show malicious-traffic log
Mar 16 18:05:43.000: [0001][3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0001] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02
-> 00:30:88:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
```

Example 1 Output Display of show malicious-traffic log Command

The following example displays output from the **show malicious log** command for IPv6 traffic. In the first line of the output, the context ID `[0001]` and the circuit handle `3/8:511:63:31/1/1/9]` are in bold. This data indicates from which context and circuit the malicious traffic was detected and dropped.

```
Aug 24 14:10:22.000: [0001] [3/8:511:63:31/1/1/9] [inv L4 cksum] Length 82  00:00:15:01:01:02 ->
00:30:88:12:78:ac IPv6 payload_length 28 hop_limit 63 3000:0:1::2.100 -> 3000:0:1::1.1019: udp length 20
Aug 24 14:10:22.000: [0001] [3/8:511:63:31/1/1/9] [inv L4 cksum] Length 82  00:00:15:01:01:02 ->
00:30:88:12:78:ac IPv6 payload_length 28 hop_limit 63 3000:0:1::2.100 -> 3000:0:1::1.1019: udp length 20
Aug 24 14:10:22.000: [0001] [3/8:511:63:31/1/1/9] [inv L4 cksum] Length 82  00:00:15:01:01:02 ->
00:30:88:12:78:ac IPv6 payload_length 28 hop_limit 63 3000:0:1::2.100 -> 3000:0:1::1.1019: udp length 20
Aug 24 14:10:22.000: [0001] [3/8:511:63:31/1/1/9] [inv L4 cksum] Length 82  00:00:15:01:01:02 ->
00:30:88:12:78:ac IPv6 payload_length 28 hop_limit 63 3000:0:1::2.100 -> 3000:0:1::1.1019: udp length 20
Aug 24 14:10:22.000: [0001] [3/8:511:63:31/1/1/9] [inv L4 cksum] Length 82  00:00:15:01:01:02 ->
00:30:88:12:78:ac IPv6 payload_length 28 hop_limit 63 3000:0:1::2.100 -> 3000:0:1::1.1019: udp length 20
Aug 24 14:10:22.000: [0001] [3/8:511:63:31/1/1/9] [inv L4 cksum] Length 82  00:00:15:01:01:02 ->
00:30:88:12:78:ac IPv6 payload_length 28 hop_limit 63 3000:0:1::2.100 -> 3000:0:1::1.1019: udp length 20
```

Example 2 Output Display of show malicious-traffic log Command

The following example displays output from the **show malicious log file** command. In the first line of the output, the context ID `[0002]` and the circuit handle `3/8:1023:63/1/1/20510]` are in bold. This data indicates from which context and circuit the malicious traffic was detected and dropped:

```
[local]Redback#show malicious-traffic log file maltrafficfile1
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
Mar 16 18:05:43.000: [0002] [3/8:1023:63/1/1/20510] [inv ip vers] Length 252  00:00:0a:01:01:02 -> 00:30:8
8:12:78:ac (1500 00ee 0000 0000 4011 e3fb c001 0102 0500 0001)
```

Example 3 Output Display of show malicious-traffic log file Command

The following example displays output from the **show malicious-traffic counters** command:

```
[local]Redback#show malicious-traffic counters
Context Name        : local             Context ID          : 0x40080001
Alarm Raised        : N                 Next Counter Update : 59 secs.

Total Malicious Pkts: 224

Malformed-IP        : 224                Malformed-L4        : 0
 Invalid IP Length  : 0                 Invalid Checksum    : 0
 Invalid IP Checksum: 0                 Invalid L4 Length   : 0
 Invalid IP Version : 0
 Invalid IP Options : 224

Filtered            : 0                 Spoofed             : 0
 Filtered Drops     : 0                  RPF Failures       : 0
                                         Null Route         : 0

Reassembly          : 0                 Other               : 0
 Reassembly Failures: 0                  Realm Drops        : 0
```

Example 4 Output Display of show malicious-traffic counters Command

7 Configuration Examples

The following example shows a complete SmartEdge router configuration that includes malicious traffic detection and monitoring configurations. The sections relating to malicious traffic detection and monitoring are highlighted in bold and commented (using the exclamation mark (!)). The configuration tasks associated with these configurations are documented in Table 3, Table 5, and Table 6:

```
!
!
service multiple-contexts
!
!
context local
!
 no ip domain-lookup
!
 interface media1 loopback
  ip address 5.0.0.1/32
!
 interface i
  ip address 1.1.1.1/21
  ipv6 address 1000:1:2:3::/64
!
 interface mgmt
  ip address 10.12.213.1/21
!
interface subs multibind
  ip address 15.1.1.1/21
  ipv6 address 2001:a:b::/48
  ip verify unicast source reachable-via any
  ip pool 15.1.0.0/21
  ipv6 pool 2001:a:b:1::/64 2001:a:b:100::/64

!
 !Apply an IPv6 ACL to an interface bound to a port and enable the counting of packets that pass
!through the filter:
interface traf
  ipv6 address 8800:1:1::/64
  ipv6 access-group aclIPv6 in count


 interface user1
  ip address 192.1.1.1/16
!Configure to perform an RPF check to verify the source IP address on all incoming unicast packets
!on the specified interface:
ip verify unicast source reachable-via any

!Apply IP ACL "acl_list" to packets associated with this circuit:
ip access-group acl_list in log

 interface user2
  ip address 14.1.1.1/16
 logging console

!Enable malicious traffic logging to a local binary file:
logging malicious-traffic file /md/mal_cxt1

!Enable malicious traffic logging to a local text file:
 logging malicious-traffic file text /md/mal_txt

!Enable malicious traffic logging to a syslog server:
 logging malicious-traffic syslog 1.1.1.1 facility local7

!Enable logging of a specified category of malicious traffic; Here the category of all is
!specified meaning all malicious packets are to be logged:
```

```
logging malicious-traffic category all

!
!Configure an IPv4 ACL:
ip access-list acl_list
  seq 10 deny tcp any any invalid-tcp-flags
  seq 20 deny ip any ip-options
  seq 30 deny udp any fragments
  seq 40 permit ip any any

!Configure an IPv6 ACL:
ipv6 access-list aclIPv6
  seq 10 deny tcp any any invalid-tcp-flags
  seq 30 deny udp any fragments
  seq 35 deny icmp any any icmp-type echo-request
  seq 40 permit ip any any


!Apply the IPv6 filtering ACL to this context (context local):
  ipv6 admin-access-group aclIPv6 in

!Configure malicious traffic parameters for this context (context local):
 malicious-traffic

!Enable counters for packets dropped due to malicious traffic:
  counters

!Enable an alarm to be generated when the counters reach configured thresholds:
  alarms
!
!
 enable encrypted 1 $1$........$kvQfdsjs0ACFjeDxQ7n/o.
!
 aaa authentication administrator local
 aaa authentication subscriber none

!
 administrator abcd encrypted 1 $1$........$Vd/KhZ/qPgvif4Gc0sf.u.
   privilege start 15
   privilege max 15
 administrator test encrypted 1 $1$........$kvQfdsjs0ACFMeDHy7n/o.
!
!As part of your default subscriber profile configuration, enable source-address validation on
!IPv4 and IPv6 traffic:
 subscriber default
   ip address pool
   ip source-validation
   ipv6 nd-profile nd1
   ipv6 source-validation
!
 ip route 10.0.0.0/8 10.12.208.1
 ip route 10.0.0.0/8 10.13.175.254
 ip route 155.53.0.0/16 10.12.208.1
 ip route 155.53.0.0/16 10.13.175.254
!
context 2
!
 no ip domain-lookup
!
 interface user_cxt2
  ip address 15.1.1.1/16
 no logging console
!Enable malicious traffic logging to a local binary file:
logging malicious-traffic file /md/mal_cxt2

!Enable logging of a specified category of malicious traffic; Here the category of filtered is specified:
logging malicious-traffic category filtered
!
 !Configure malicious traffic parameters for this context (context 2):
 malicious-traffic

!Enable counters for packets dropped due to malicious traffic:
  counters

!Enable an alarm to be generated when the counters reach certain thresholds:
```

```
  alarms

!
!
context 3
!
 no ip domain-lookup
!
 interface user_cxt3
  ip address 16.1.1.1/16
 no logging console
 !Enable malicious traffic logging to a local binary file:
logging malicious-traffic file /md/mal_cxt3

!Enable logging of a specified category of malicious traffic;
!Here the category of failed-reassembly is specified:
logging malicious-traffic category failed-reassembly
!
!Configure malicious traffic parameters for this context (context 3):
malicious-traffic

!Enable counters for packets dropped due to malicious traffic:
  counters

!Enable an alarm to be generated when the counters reach certain thresholds:
  alarms
!
!
! ** End Context **

 logging tdm console
 logging active
 logging standby short
!
!
!Enable the SNMP server
snmp server enhance ifmib
 traps ifmib ip
snmp view eye-view internet included
snmp community public all-contexts view eye-view read-write
snmp target ser 10.12.213.3 port 12612 security-name public version 2c view eye-view
!
 system clock timezone PST -7 0 local
!
!
!At the global level, configure alarm parameters for malicious traffic:
malicious-traffic
!
!Specify the rate and burst limits for malicious traffic log events:
logging rate-limit 100 burst 5000
!
!Configure global alarm parameters:
alarms
!
!Configure the amount of time between the reporting of malicious-traffic counters:
  interval 80
!Specify the high and low threshold values (in packets) for malicious traffic alarms:
  threshold high 2000 low 1000
!
card ge4-20-port 1
!
card ge-10-port 3
!
port ethernet 3/3
 no shutdown
 bind interface user2 local
!
port ethernet 3/8
 no shutdown
 encapsulation dot1q
 bind interface user1 local
 dot1q pvc 2
  bind interface user_cxt2 2
 dot1q pvc 3
  bind interface user_cxt3 3
!
```

```
!
port ethernet 7/1
! XCRP management ports on slot 7 and 8 are configured through 7/1
 no shutdown
 bind interface mgmt local
!
port ethernet 9/3
 no shutdown
 encapsulation pppoe
 bind authentication pap maximum 50
!
 system hostname isram6
!
 boot configuration /flash/admin.cfg
 no timeout session idle
!
no service console-break
!
service crash-dump-dram
!
no service auto-system-recovery
!
end
```

Reference List

[1] *SmartEdge Border Gateway Function*, 155 13-CRA 119 1170/1 Uen