Syslog and the Barracuda Email Security Gateway

https://campus.barracuda.com/doc/12193950/

Information Provided by the Syslog

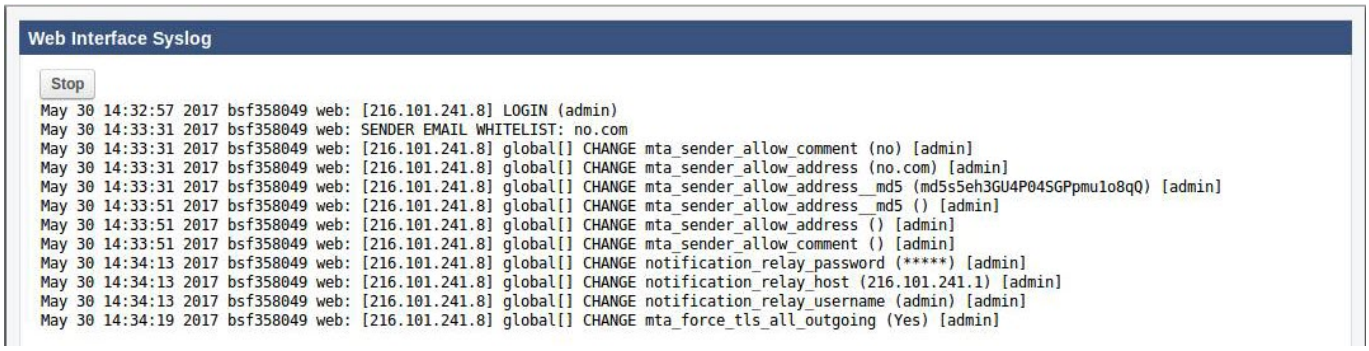
The Barracuda Email Security Gateway generates syslog messages as a means of logging both changes to the web interface configuration and what happens to each message as it is processed. The syslog messages are stored in text file format on the Barracuda Email Security Gateway and can be sent to a remote server configurable by the administrator. There are two syslog outputs you can monitor:

- The *Web* syslog logs user login activities and any configuration changes made to the Barracuda Email Security Gateway web interface. User activity data appears on the local facility with login information at the *info priority level*, and configuration changes appear at the *debug priority* level on the specified syslog server. See the **Syslog** section of the **ADVANCED > Troubleshooting** page for the facility to open a browser window and view the *Web* syslog output.
- The *Mail syslog* logs what happens to each message as it is processed and is presented in a raw data format that includes reason codes relative to the message process. This guide will help you understand, parse, and utilize the mail syslog messages and reason codes generated by the Barracuda Email Security Gateway.

Parsing the Web Syslog

On the **ADVANCED > Troubleshooting** page, click **Monitor Web Syslog** in the Syslog section of the page. The format of the Barracuda Email Security Gateway syslog output is detailed below.

Timestamp	Host	Syslog	Client IP	Scope of variable	Action	Config variable	Setting	Login
May 30 14:34:19 2017	bsf358049	web:	[216:101.241.8]	global	CHANGE	mta_force_tls_all_outgoing	Yes	admin



Configuring the Barracuda Mail Syslog

To configure the *Mail* syslog, using the Barracuda Email Security Gateway web interface, navigate to the **ADVANCED > Advanced Networking** page and enter the IP address and port of the syslog server to which syslog data related to mail flow should be sent. You can also specify the protocol – TCP or UDP – over which syslog data should be transmitted. TCP is recommended.

Syslog data is the same information as that used to build the Message Log in the Barracuda Email Security Gateway and includes data such as the connecting IP Address, envelope 'From' address, envelope 'To' address, and the spam score for the messages transmitted. This syslog data appears on the mail facility at the debug priority level on the specified syslog server. As the Barracuda Email Security Gateway uses the syslog messages internally for its own message logging, it is not possible to change the facility or the priority level. See the **Syslog** section of the **ADVANCED > Troubleshooting** page in the Barracuda Email Security Gateway web interface to open a window and view the Mail syslog output.

If you are running syslog on a UNIX machine, be sure to start the syslog daemon process with the “-r” option so that it can receive messages from sources other than itself. Windows users will have to install a separate program to utilize syslog since the Windows OS doesn’t include syslog capability. Kiwi Syslog is a popular solution, but there are many others are available to choose from, both free and commercial.

Syslog messages are sent via either TCP or UDP to the standard syslog port of 514. If there are any firewalls between the Barracuda Email Security Gateway and the server receiving the syslog messages, make sure that port 514 is open on the firewalls.

Parsing the Mail Syslog

The format of the Barracuda Email Security Gateway syslog output is detailed below. For a programmer's guide to parsing the syslog, see How to Parse the Barracuda Email Security Gateway Syslog.

Timestamp	Host	Barracuda Process	Client IP	Message ID	Start	End	Service	Info
Sep 8 17:38:48 2013	dev1	inbound/pass1	XX.XX.XX.XX	1126226282-27564-2-0	1126226286	1126226328	RECV	[.....]

Barracuda Syslog Format

The Barracuda Email Security Gateway sends syslog messages in the following format. Whenever an

action is taken on a message, it is logged with the syslog. A message sent to multiple recipients will be logged separately for each recipient. Please be aware that the various syslog implementations may not display the messages in this exact format. However, the sections should still be present in the syslog lines as shown in the table below. The following represents the main part of the syslog line:

Each section of the syslog line is defined in the table below.

Syslog Section	Description
Timestamp	The time that the syslog message was logged. For reporting purposes, this section of the syslog line can be ignored. It is useful when analyzing the logs by hand, but is not needed for compiling reports. Note: In version 5.1.3.007, the Year was appended to the end of the Timestamp field.
Host	Indicates the host that generated the syslog message. Useful if you have multiple Barracuda Networks appliances and need to know which host sent the message.
Barracuda Process	Indicates the process that the email message was in when the syslog message was generated. Possibilities are: inbound/pass1 ... inbound/pass2 ... scan ... outbound/smtp. Note: In version 6.0.2.002, the 5 digit Process ID (**[27564]** in the example above) was removed.
Barracuda Message ID	The most important piece of the syslog entry. This ID is used to uniquely identify a message. The ID may occur in one of two formats (a different format is used for the inbound process and for the scan process). For example, this ID 1126226282-27564-2-0 is used for RECV transactions and it means the following: 1126226282 = UNIX timestamp 27564-2= Internal Process ID 0 = Message number in SMTP session – this number indicates how many messages have been sent in that single SMTP session
Start	The start time of the message in UNIX timestamp format, indicating when the sender began giving us the “From” information for the message.
End	The end time of the message in UNIX timestamp format, indicating when the sending server terminated sending of the message.
Service	The service that produced the message. The following services are available: • **RECV –** This service indicates a message was handled by the MTA and processing stopped. • **SCAN –** This service indicates the message was scanned and processing may have stopped or it may have been sent to the outbound processing for delivery. • **SEND –** This service indicates status of outbound delivery. It is the only message that may appear multiple times for a given message ID since delivery may initially have been deferred before succeeding later on.

Info	This section contains the actual information about what happened to a given message. It is dependent on the service that sent the information, and the following formats are used: • **RECV –** Sender Recipient Action Reason ReasonExtra • **SCAN –** Encrypted Sender Recipient Score Action Reason ReasonExtra SZ "SUBJ:"Subject Note that if TLS is used, then '**ENC**' will be displayed before the **SZ**: entry; if TLS is not USED, there will be a '**–**' before the **SZ**: entry. • **SEND –** Encrypted Action QueueID Response The possible fields have the following meanings: • **Sender –** The address of the sender, if available, and '**–**' if the SENDER is blank. • **Recipient –** The address of the recipient if available and, '-' if not available. • **Action –** The action code indicating what action was taken for the message. For the "SEND" service these action codes have different meanings. • **Reason –** The reason code indicating the reason for the taken action. • **ReasonExtra –** Extra information about a given reason (e.g. the RBL or the body filter that matched in the message). • **Encrypted –** Indicates whether or not the message was received or sent encrypted. • **Score –** The score given to the message if the scoring mechanism was run. • **Subject –** The subject of the message if it was available. • **QueueID –** The queue ID of the message on the Barracuda as delivery is being attempted. • **Response –** The response given back by the mail server if available.

Barracuda Action Codes

RECV and SCAN Services

ID	Meaning
0	Allowed Message
1	Aborted Message
2	Blocked Message
3	Quarantined Message
4	Tagged Message
5	Deferred Message
6	Per-User Quarantined Message
7	Allow Listed Message
8	Encrypted Message
9	Redirected Message

10	Attachments Stubbed*

* Applies to version 6.0 and higher

SEND Service

ID	Meaning
1	Delivered Message
2	Rejected Message
3	Deferred Message
4	Expired Message

Barracuda Reason Codes

RECV and SCAN Services

ID	Meaning
1	Virus
2	Banned Attachment
3	RBL Match
4	Rate Control
5	Too Many Message In Session
6	Timeout Exceeded
7	No Such Domain
8	No Such User
9	Subject Filter Match
11	Client IP
12	Recipient Address
13	No Valid Recipients
14	Domain Not Found
15	Sender Address
17	Need Fully Qualified Recipient
18	Need Fully Qualified Sender
19	Unsupported Command
20	MAIL FROM Syntax Error
21	Bad Address Syntax
22	RCPT TO Syntax Error

23	Send EHLO/HELO First
24	Need MAIL Command
25	Nested MAIL Command
27	EHLO/HELO Syntax Error
30	Mail Protocol Violation
31	Score
34	Header Filter Match
35	Sender Block/Accept
36	Recipient Block/Accept
37	Body Filter Match
38	Message Size Bypass
39	Intention Analysis Match
40	SPF/Caller-ID
41	Client Host Rejected
44	Authentication Not Enabled
45	Allowed Message Size Exceeded
46	Too Many Recipients
47	Need RCPT Command
48	DATA Syntax Error
49	Internal Error
50	Too Many Hops
51	Mail Protocol Error
55	Invalid Parameter Syntax
56	STARTTLS Syntax Error
57	TLS Already Active
58	Too Many Errors
59	Need STARTTLS First
60	Spam Fingerprint Found
61	Barracuda Reputation Allow List
62	Barracuda Reputation Block List
63	DomainKeys
64	Recipient Verification Unavailable
65	Realtime Intent
66	Client Reverse DNS
67	Email Registry
68	Invalid Bounce

69	Intent - Adult
70	Intent - Political
71	Multi-Level Intent
72	Attachment Limit Exceeded
73	System Busy
74	BRTS Intent
75	Per Domain Recipient
76	Per Domain Sender
77	Per Domain Client IP
78	Sender Spoofed
79	Attachment Content
80	Outlook Add-in
82	Barracuda IP/Domain Reputation
83	Authentication Failure
85	Attachment Size
86	Virus detected by Extended Malware Protection **
87	Extended Malware Protection engine is busy **
88	A message was categorized for Email Category**
89	Macro Blocked*

* Applies to version 8.0.1 and higher

** Applies to version 6.1 and higher

***With version 7.1.1, no longer used

****Applies to version 7.1.1.002 and higher

Figures