CYREN IP Reputation (ctIPd) Daemon Reports

Contacts

Any technical questions you or your developers have about using the ctwsd should be addressed to support@cyren.com.

About CYREN

CYREN™ provides proven Internet security technology to more than 150 security companies and service providers including 1&1, Check Point, F-Secure, Google, Microsoft, Panda Security, Rackspace, US Internet, and WatchGuard, for integration into their solutions. CYREN's GlobalView™ and patented Recurrent Pattern Detection™ (RPD™) technologies are founded on a unique cloud-based approach, and protect effectively in all languages and formats. CYREN Antivirus utilizes a multi-layered approach to provide award winning malware detection and industry-leading performance.

CYREN technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, enabling our partners to protect end-users from spam and malware, and ensure safe, compliant browsing. The company's expertise in building efficient, mass-scale security services mitigate Internet threats for thousands of organizations and hundreds of millions of users in 190 countries.

CYREN, formerly known as Commtouch, was founded in 1991, is headquartered in the US in McLean, Virginia, with offices in Palo Alto, California, Herzliya, Israel, Berlin, Germany, and Reykjavik, Iceland.

For more information about enhancing security offerings with CYREN technology, visit our website at www.cyren.com, see our blog at http://blog.cyren.com or write to support@cyren.com.

Trademark and Copyright Statement

Table of Contents

1 Introduction

The CYREN GlobalView Mail Reputation daemon (**ctIPd**™) includes a built-in capability to enable it to generate reports on the daemon's activities and performance based on time, actions, or a specific IP address or group of addresses. The command line reports initiate scripts to query ctIPd's internal logfiles and generate a predefined selection of data. The following ctIPd reports are available:

get_tran: output one or more transactions from the logfile for any given value according to transaction ID (ctid value) or IP address (or group of addresses).

get_action: display all the transactions for one or more predefined IP addresses within a predefined time period filtered for any predefined call-to-action (accept, tempfail, permfail).

get_stats: generate statistics for a predefined period of time for all or selected IP addresses with a daily breakdown or for the entire period.

Generating reports using ctIPd's internal reporting feature involves the following two steps:

Enabling ctIPd's logging functionality

Generating reports from the command line

These steps are explained in detail in this document. It is highly recommended that you read the following documents before configuring and generating reports:

ctIPd Product Description

ctIPd Implementation Guidelines

ctIPd Integration Guide

1.1 Additional Resources

In addition to this document, the following additional resources are available within the ctIPd package:

ctIPd Product Description

ctIPd Implementation Guidelines

ctIPd Integration Manual

ctIPd Testing and Evaluation Guidelines

2 Enabling Logging

A default configuration file is provided with the ctIPd package containing the necessary configuration parameters for the daemon. Most of the parameters in the configuration file are optional, and have default values that are enforced if another value is not specified. For a full explanation of the configuration file, refer to the *ctIPd Integration Manual*.

To enable you to generate reports based on ctIPd's performance, you must enable ctIPd's logging functionality, which is deactivated by default. These logs maintain records for all transactions between ctIPd and the querying device, including its resulting analysis and call-to-action. This activity is controlled by the Log Server component. Until this component is activated, ctIPd does not log its activities and therefore cannot generate the reports discussed in the following sections. Therefore, the initial step in producing reports is first to enable the Log Server. This is done via the ctipd.conf file. The logfiles are created only for the purpose of reporting and use an internal syntax that ctIPd uses to compile the reports. Some options are configurable (such as the location, size of each file, reporting period, etc.). These are detailed in the *ctIPd Integration Manual*.

2.1 Initiating the Logging Functionality

You can enable the logging function by configuring the ctipd.conf file's [LogServer] section.

To prompt ctIPd to begin maintaining logs:

1. In the LogServer section of the ctipd.config file, change the value of `LogMethod to 1.` The default value is `0`, meaning that no logging is performed.
2. Modify the options related to the log maintenance option. These include:

Option	Explanation
DirName	The `DirName` option specifies the directory name where the logfiles are located. By default, the files are stored in the /tmp/ctipd_log directory.
DaemonName	The name of the daemon for which logs are kept. In multi-daemon deployments, each daemon should be given a unique name, if you wish to generate meaningful reports according to daemon name.
MaxSize	The `MaxSize` option specifies the maximum storage size to allocate to all the logfiles. Once this limit is reached, older files are deleted as necessary to enable writing new files. The default value is `2000` MB.

Option	Explanation
MaxPeriod	The `MaxPeriod` option specifies the period of time to keep logfiles. Any logfile with older creation date will be deleted from the storage. The default value for this option is 24 hours.
MaxFileSize	The `MaxFileSize` option determines the maximum file size for any logfile. As soon as this value is reached, the file that is currently open for writing new records is closed and written to the storage, while a new logfile is created to begin logging data. The default value for the maximum logfile size is `50` MB.
Host	This option refers to the host name into which logfiles are saved. By default, this option is set to `localhost`, but if access permissions are set correctly the logfiles can be saved to a remote host.
Port	The `Port` option indicates the port via which logging data is transmitted. The default value is: `23456.`
BindingAddress	The `BindingAddress` option defines the address to be bound to the socket. The default address is `INADDR_ANY`.

3. Restart the daemon.

Once you restart the daemon, logging is enabled and the logs will automatically be generated to a predetermined location according to the parameters you defined in the configuration file.

Note: *For more information on the configuration file and options related to configuring the logging functionality, see Enabling Logging.*

Each instance of ctIPd logs its own transactions to a local logfile, adding a unique daemon-id to the name of the file. Reports from multiple daemons can then be collected by a separate application to a designated location, typically a subfolder in the directory where one of the daemons stores its logfiles. You can then run one of the reporting scripts on the root directory to create an aggregated report of multiple ctIPd activity.

3 Generating Reports

ctIPd reports are generated from the command line by initiating one of the following scripts:

```
get_tran.pl
get_action.pl
get_stats.pl
```

The syntax used to run the scripts is as follows:

```
<script name> <parameters> <directory name>
```

The <script name> specifies which report will be generated.

One or more <parameters> can be added following the script name. Each parameter is separated by a space. In the following sections, each report and its possible parameters are detailed.

Note: *Some of the parameters are mandatory and must be specified to generate a report successfully.*

Specify the <directory name> where the logfiles are stored. This is the `DirectoryName` value from the `ctipd.conf` file. This is a required parameter.

3.1.1 General Report Parameters

Some of the parameters, like the time value, are identical for all reports, while others are unique to a particular report. The time value, a generic parameter, is explained in the following section.

3.1.1.1 Report Time Values

To generate the various reports effectively, you must specify time values, as follows:

The minimum time (--mintime) value details the starting point for the report.

The maximum time (--maxtime) value details the ending point for the report.

Therefore, the maxtime must always be a smaller value (closer to the current time) than the mintime.

You can use either absolute values for a time and date, or use values relative to the current time. The following syntax should be used:

```
--mintime '<value>' or --maxtime '<value>'
```

The following table details the possible options for values that can be used in the above syntax.

Value	Example
YYYY-MM-DD hh:mm:dd	2008-03-30 15:28:46
$now	Indicates current time. You can add integers to modify the time. For example: `--mintime '$now-2*$hour'` means that the report should begin now minus 2 hours (or 2 hours ago)
$minute	Indicates a value in minutes. For example: `--maxtime '$now-15*$minute'` means that the ending time for the report is now minus 15 minutes (or 15 minutes ago)
$hour	Indicates a value in hours and can be used in the previous examples.
$day	Indicates a value in days and can be used as in the previous examples.

3.1.2 Multi-Daemon Reports

It is possible to produce reports that display information and transactions related to more than one daemon by placing the logging files from multiple daemons in one directory and running the scripts. Note that if you choose to do this, it is important to configure each daemon with a unique daemon name in the ctipd.conf file. By default, this option is set to 0001. If this is not modified, all daemons using this configuration file would have the same name and the logging files, once combined into a single directory would not be able to differentiate between the various daemons.

To modify the daemon name:

1. In the LogServer section of the ctipd.config file, change the value of DaemonName. The default value is `0001`. Each daemon in the organization should be given a unique ID (can be a combination of letters and/or numbers).
2. Restart the daemon.

To generate reports for several daemons, place the log files from some or all of the daemons in the organization in a central location and then follow the instructions detailed in the following sections, according to which report you wish to produce.

4 Transaction Reports

The *get_tran* report generates a report about one or more specified transactions based on information extracted from the log files that are maintained by ctIPd. To generate the report, you must provide one of the following parameters and then specify the report date and time criteria:

The ctid (ctIPd transaction ID). This value can be found in the RefID number returned with each query response.

A single IP address and a time period. When using this option, all transactions for the specified IP address within the specified time period are sent to stdout.

Note: *You must specify a mintime or you will get an error.*

You can specify additional IP address, by inserting a comma after the IP address and adding another. For example, `216.163.176.201, 216.163.176.202, 216.163.176.203 etc.`

To customize the get_tran report, you can use the following parameters:

Parameter	Description
--ctid or --ip	You must specify either the ctid value of the desired transaction or one or more IP addresses. You can specify more than one IP address by using commas to separate each IP or IP range.
--mintime	This is the starting value (date and time) of the report. The report will begin at this time and continue until the –-maxtime value. For an explanation and example of acceptable time-related values, see Report Time Values.
--maxtime	This is the ending value (date and time) of the report. If no –-maxtime value is specified, the report will include all related data until “now” (the current time). For an explanation and example of acceptable time-related values, see Report Time Values.
--force	ctIPd cannot scan an open log file that is currently being used to collect ongoing data. You can use the --force command to force ctIPd to close the open file so that it can be scanned. A new log file will be opened so that ongoing queries are still logged.
--sort	Enables you to generate the report with the information sorted by IP address.
--help	Displays the Help information detailing script parameters.

4.1.1 Script Syntax Sample

Following is an example of a `get_tran` script call that would initiate a transaction report on any transactions from IP address 216.163.176.213, including:

- The reporting period will begin on `2008-04-06` (April 6, 2008) at 15:25:00 and end on `2008-04-06` at 23:59:59.
- The report will get transactions related to IP address: 216.163.176.210.
- The logs used to generate this report will be found in the `/tmp/reports` directory. The report itself is stdout.

Within the specified period of time, each individual query for the specified IP address is listed.

Example

```
./get_tran.pl --ip 216.163.176.210 --mintime "2008-04-06 15:25:00" --
maxtime "2008-04-06 23:59:59” tmp/reports
```

4.1.2 get_tran Output Sample

Following is a sample output for the get_tran report. Below the example is a line-by-line explanation of each entry. Note that in this sample, two transactions are identified (the F: indicates the last line of the each entry, and the H:8 indicates the beginning of the next record).

```
H:8,2008-04-06
15:25:00,0001,1207495500.7F000001.00149,0001.AC141447.47F8EE2F.
0013,0,216.163.176.210,100,,G3,95,0,,,0,
R:0,G3
R:1,0,5,4
R:2,95
R:3,92,90
R:7,120
C:1,
F:
H:8,2008-04-06
15:25:00,0001,1207495500.7F000001.00177,0001.AC141447.47F8EE2F.
0013,0,216.163.176.210,100,,G3,95,0,,,0,
R:0,G3
R:1,0,5,4
R:2,95
R:3,92,90
R:7,120
C:1,
F:
```

4.1.3 get_tran Output Explanation

The `get_tran` output is divided into three sections, as follows:

H:8	Details the most used values, including the timestamp, daemon name, transaction number, queried IP and much more. For more details, see H:8 Data Options.
R:x	Details the raw reputation data values for each data type. For more information, see R Data Options.
C	Details data related to some counters. For more information, see C Data Options.
F:	Delimiter to separate between various transactions

The final line of the report is marked by the F to indicate the report's final line. The information for each of the sections is detailed in the following sections.

4.1.4 H:8 Data Options

The H:8 header line is typically the longest line of the report, and the one that contains the most amount of valuable and often-used information. Each value is separated by a comma and correlates (in order) to the following values.

Example	Value	Explanation
2008-02-19 07:40:52	ts	Timestamp, including the date and hour the report was created.
0001	dn	The ctIPd daemon ID number.
1203406852.7F000001.2	ctid	The ctIPd transaction number.
0001.0A0B0302.47BA89D4.0019	tid	The CYREN Resolver transaction number.
1	fc	Flag indicating whether the recommendation was taken from the local cache, as follows: • 0=No • 1=Yes
`216.163.176.210`	ip	The IP address being queried.
201	dm	Flag indicating whether the decision managing options are enabled and what the recommended action is. For more information, see Action Codes.

Example	Value	Explanation
1203406852	fs	Indicates when this IP was first queried. Time represented in seconds from epoch.
T2	ipc	IP Class
66	rsk	Risk Level
0	pt	Protocol type. Options include: • 0=HTTP • 1=UDP
0	zl	Zero latency enabled, as follows: 0=No; 1=Yes. When OEM sends query,
0	cl	cl = <child license key in authenticated mode: license[:oem token]>

4.1.4.1 R:x Data Options

The R section details the individual values per data type associated with each transaction, according to the following:

Value	Associated Data Type
0	IP Class
1	Volume
2	Risk Level
3	Spam Ration
4	Bulk Ratio
5	24h
6	Maximum Hits
7	Time to Live (TTL)

4.1.4.2 C Data Options

C – Internal Counters Decision Manager

5 Call-to-Action Reports

The *get_action* report focuses on the call-to-action responses issued by ctIPd. The objective is to show all the transactions for one or more predefined IP addresses within a predefined time period for a predefined action (accept, tempfail, permfail).

Note: *This report is not applicable if you have disabled the decision manager feature.*

You can specify additional IP address, by inserting a comma after the IP address and adding another. For example, `216.163.176.201, 216.163.176.202, 216.163.176.203 etc.`

To generate the report, you can provide the IP address and the specific action. If no transaction is found, an error message is returned. To customize the `get_action` report, you can use the following parameters:

Parameter	Description
--ip	You can specify one or more IP addresses. To specify more than one IP address, use a comma between each additional IP address.
--dmaction	Specify one of the following actions: ▪ accept ▪ permfail ▪ tempfail ▪ tempfthrottle ▪ acceptthrottle For more information, see dmaction Options.
--mintime	This is the starting value (date and time) of the report. The report will begin at this time and continue until the –-maxtime value. For an explanation and example of acceptable time-related values, see Report Time Values.
--maxtime	This is the ending value (date and time) of the report. If no –-maxtime value is specified, the report will include all related data until “now” (the current time). For an explanation and example of acceptable time-related values, see Report Time Values.

Parameter	Description
--force	ctIPd cannot scan an open log file that is currently being used to collect ongoing data. You can use the --force command to force ctIPd to close the open file so that it can be scanned. A new log file will be opened so that ongoing queries are still logged.
--sort	Enables you to generate the report with the information sorted by IP address.
--help	Displays the Help information detailing script parameters.

5.1.1 dmaction Options

You can specify one of the following dmactions:

Action	Report Displays Records for All Recommendations to
Accept	Accept the connection
Permfail	Permanently refuse the connection
Tempfail	Temporarily refuse the connection
Tempfthrottle	Temporarily refuse the connection (during throttling)
Acceptthrottle	Accept the connection (during throttle)

5.1.2 Script Syntax Sample

Following is an example of a get_action script call that would initiate a report based on the following criteria:

A report on any transaction that resulted in an accept from IP address 216.163.176.213.

Note: You can specify more than one action per report by using the following syntax: --dmaction accept, tempfail

The reporting period will begin on `2008-04-06` (April 6, 2008) at 15:25:00 and end on `2008-04-06` at 23:59:59.)

The logs used to generate this report will be found in the `/tmp/reports` directory. The report itself is stdout.

Example:

```
./get_action.pl --ip 216.163.176.210 --mintime "2008-04-06 15:25:00"
--maxtime "2008-04-06 23:59:59" --dmaction accept tmp/
```

5.1.3 get_action Output Sample

```
216.163.176.210,2008-04-06 15:25:00,100,1207495500.7F000001.00149
216.163.176.210,2008-04-06 15:25:00,100,1207495500.7F000001.00177
216.163.176.210,2008-04-06 15:25:00,100,1207495500.7F000001.00205
216.163.176.210,2008-04-06 15:25:01,100,1207495501.7F000001.00233
216.163.176.210,2008-04-06 15:25:01,100,1207495501.7F000001.00261
216.163.176.210,2008-04-06 15:25:01,100,1207495501.7F000001.00289
216.163.176.210,2008-04-06 15:25:02,100,1207495502.7F000001.00317
216.163.176.210,2008-04-06 15:25:02,100,1207495502.7F000001.00345
216.163.176.210,2008-04-06 15:25:03,100,1207495503.7F000001.00373
216.163.176.210,2008-04-06 15:25:03,100,1207495503.7F000001.00401
216.163.176.210,2008-04-06 15:25:03,100,1207495503.7F000001.00429
216.163.176.210,2008-04-06 15:25:04,100,1207495504.7F000001.00457
216.163.176.210,2008-04-06 15:25:04,100,1207495504.7F000001.00485
216.163.176.210,2008-04-06 15:25:04,100,1207495504.7F000001.00513
216.163.176.210,2008-04-06 15:25:05,100,1207495505.7F000001.00541
216.163.176.210,2008-04-06 15:25:05,100,1207495505.7F000001.00569
216.163.176.210,2008-04-06 15:25:06,100,1207495506.7F000001.00597
216.163.176.210,2008-04-06 15:25:06,100,1207495506.7F000001.00625
216.163.176.210,2008-04-06 15:25:06,100,1207495506.7F000001.00653
```

5.1.4 get_action Output Explanation

Each line of the report offers information about a single transaction that resulted in the specified action within the specified period of time. The following table explains a single line in the above sample:

Example	Explanation
`216.163.176.210`	IP address for the record
`2008-04-06 15:25:06`	Time stamp for the transaction
`100`	ctIPd coded value for the action. For more information, see Action Codes.
`1207495506.7F000001.00653`	The ctIPd transaction number.

Action Codes

The following tables details the actions that ctIPd may display in the get_action report, and the associated codes.

Action	Code
Accept	100,101
Accept during throttle period	102
Tempfail	200, 201
Tempfail during throttle period	202
Permfail	300

6 Statistic Reports

The *get_stats* report provides statistics on one or more predefined IP addresses over a given period of time. To generate the report, you must provide at least one IP address and a time period.

Note: *You can specify additional IP address, by inserting a comma after the IP address and adding another. For example,* `216.163.176.201, 216.163.176.202, 216.163.176.203 etc.`

If no transaction is found, an error message is returned. To customize the get_stats report, you can use the following parameters:

Parameter	Description
--ip	You must specify one or more IP addresses. You can specify more than one IP address by using commas to separate each IP or IP range.
--general	Creates a report for the entire period as a single time block.
--day	Creates a daily report of statistics for the specified period
--mintime	This is the starting value (date and time) of the report. The report will begin at this time and continue until the –-maxtime value. For an explanation and example of acceptable time-related values, see Report Time Values.
--maxtime	This is the ending value (date and time) of the report. If no –-maxtime value is specified, the report will include all related data until “now” (the current time). For an explanation and example of acceptable time-related values, see Report Time Values.
--force	ctIPd cannot scan an open log file that is currently being used to collect ongoing data. You can use the --force command to force ctIPd to close the open file so that it can be scanned. A new log file will be opened so that ongoing queries are still logged.
--sort	Enables you to generate the report with the information sorted by IP address.
--help	Displays the Help information detailing script parameters.

6.1.1 Script Syntax Sample

Following is an example of a get_stats script call that would initiate a report based on the following criteria:

A report on any transaction from IP address 216.163.176.213.

The report will begin on January 2, 2008 at 15:25:00 and end at the current time, since only a –mintime was specified in the cmd line

The logs used to generate this report will be found in the `/tmp/reports` directory. The report itself is stdout.

There are two types of reports generated for the get_stats option. These include a ---general report for a specified period and a --daily report for a specific day.

Syntax Example

```
./get_stats.pl --mintime "2008-02-01 15:25:00" --general  --ip
216.163.176.213 tmp/
```

6.1.2 get_stats Output Sample (General)

```
216.163.176.201,11,0,0,0,0,2008-04-06 15:29:35,2008-04-06 16:10:18
216.163.176.202,0,0,0,0,13126,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.203,13125,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.204,13126,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.205,13125,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.206,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.207,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.208,13125,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.209,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.210,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.211,13122,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.212,13123,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.213,0,12945,182,0,2,2008-02-19 07:41:15,2008-04-06 15:28:01
216.163.176.214,0,90,0,13033,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.215,0,90,0,13034,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.216,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.217,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.218,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.219,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.220,13123,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.221,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.222,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.223,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.224,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.225,13123,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.226,13122,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
216.163.176.227,13122,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:07
216.163.176.228,0,12940,182,0,0,2008-04-06 11:35:04,2008-04-06 15:25:07
216.163.176.229,0,95,0,13026,0,2008-04-06 11:35:04,2008-04-06 15:25:07
```

Sample Syntax

```
./get_stats.pl --mintime "2008-02-01 15:25:00" --day --ip 216.163.176.213
tmp/
```

6.1.3 get_stats Output Sample (Day)

```
2008-04-06,216.163.176.201,11,0,0,0,0,2008-04-06 15:29:35,2008-04-06 16:10:18
2008-04-06,216.163.176.202,0,0,0,0,13126,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.203,13125,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.204,13126,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.205,13125,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.206,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.207,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.208,13125,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.209,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.210,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.211,13122,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.212,13123,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.213,0,12945,182,0,0,2008-04-06 11:35:04,2008-04-06 15:28:01
2008-04-06,216.163.176.214,0,90,0,13033,0,2008-04-06 11:35:04,2008-04-06
15:25:06
2008-04-06,216.163.176.215,0,90,0,13034,0,2008-04-06 11:35:04,2008-04-06
15:25:06
2008-04-06,216.163.176.216,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.217,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.218,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.219,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.220,13123,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.221,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.222,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.223,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.224,13124,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.225,13123,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.226,13122,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:06
2008-04-06,216.163.176.227,13122,0,0,0,0,2008-04-06 11:35:04,2008-04-06 15:25:07
2008-04-06,216.163.176.228,0,12940,182,0,0,2008-04-06 11:35:04,2008-04-06
15:25:07
2008-04-06,216.163.176.229,0,95,0,13026,0,2008-04-06 11:35:04,2008-04-06
15:25:07
```

6.1.4 get-stats Output Explanation

Example	Explanation
2008-04-06	Transaction date
216.163.176.229	IP address for the record
0	Number of accepts for the report period
12940	Number of accepts during throttle for the report period
182	Number of tempfails for the report period
0	Number of tempfails during throttle for the report period
0	Number of permfails
2008-04-06 11:35:04	Time stamp for the first transaction seen for this IP address.
2008-04-06 15:25:07	Time stamp for the last transaction seen for this IP address