ctIPd™ Testing and Evaluation Guidelines

This document presents a detailed explanation of how you can test and evaluate ctIPd within your application or network. It is designed for Product Managers, developers, and those involved in the implementation and integration of ctIPd into the OEM partner's application. References are made to other ctIPd documentation, where detailed instructions and descriptions can be found.

For a discussion on implementation options including implementation, configuration options, etc., refer to the *ctIPd Implementations Guidelines*. For a discussion on integrating ctIPd into your application, refer to the *ctIPd Integration Manual*. Additional documents are listed in a later section and detailed in the *ctIPd Getting Started* document.

This document is divided into the following sections:

- Prerequisites
- Configuration requirements for testing and evaluating ctIPd
- Testing options; determining which traffic to use for testing
- Testing process
- Understanding test results
- Reporting Cases of Reputation Mistakes

Prerequisites

Note:	*ctIPd configuration requirements are explained in the ctIPd Integration Manual. Optional configurations are also explained in the ctIPd Implementation Guidelines.*

Before testing and evaluation can take place, you will need to verify that you have received the following from CYREN:

- License key for authentication
- Server address for communicating with the CYREN Datacenter
- ClientID to include in iFrame application (if implemented)

You will also need to coordinate the following with CYREN:

- Decision Manager template to be used
- Provide a testing email account or IP address of the MX record (optional)

Decision Manager Template

By default, ctIPd returns a recommended call-to-action for each query received. ctIPd returns these recommendations based on computed reputation data available at the time of each query. The logic by which ctIPd computes recommended calls-to-action is predefined in a Decision Manager template that is downloaded from the Datacenter by ctIPd when it connects to authenticate the license key. Several different templates are available and CYREN may add new ones from time to time. Since the template is associated with the license key code, if you are deploying ctIPd for customers requiring different templates, it is recommended that for each

customer type you use a different license key code and coordinate with CYREN to associate the proper template to each key.

To determine the correct template for your needs:

1. Determine the average number of SMTP connections that the organization processes over a 24-hour period.
2. Divide this number by the number of deployed ctIPd units. This gives you the approximate number of queries that each unit is expected to process.
3. Match this number to the table below. If the default *Medium* template does not match your requirements, contact CYREN Technical Support to adjust your license key to a different template.

Number of Queries per Daemon	Appropriate Template
Under 3,000	Small
Between 3,000 and 300,000	Medium (default template)
Over 300,000	Large

By default, CYREN assigns the Medium template and no further action or adjustment is required. For more information on ctIPd's Decision Manager logic, refer to the *ctIPd Implementation Guidelines* document.

Testing email account or MX IP Record

CYREN can assist you in testing and evaluating ctIPd by passing to your application examples of email messages for which IP reputation is known. ctIPd running on your application will then evaluate these IP connection requests and the responses can be evaluated. To implement this option, you can provide CYREN with an email testing account to which to forward message sources, or give CYREN your MX IP record ID. CYREN will then forward a variety of emails to emulate sending sources.

Configuration Requirements for Testing

A full explanation of the configuration file is contained in the ctIPd Integration Manual. Following are the parameters that are required in order to test and evaluate ctIPd. These include:

- License key
- Server Address
- Protocol Issues
- Logging Method
- Proxy Settings

Each of these are detailed in the following sections and explained more thoroughly in the *ctPId Integration Manual* and/or the *ctIPd Implementation Guidelines* document.

License key

The CYREN Datacenter requires ctIPd to pass the CYREN license key code to authenticate and provide GlobalView Mail Reputation services. The license key code is added into the `LicenseKey=` parameter of the ctipd.conf configuration file. The license code is a unique key on the CYREN's database used to both authenticate the user's account and to enable the agreed-upon SLA that is sometimes different than the default

(e.g., a decision manager template ID to download as described later in this document). For more information on the license key code, refer to the *ctIPd Implementation Guidelines*.

Server Address

When communicating with the Datacenter to receive service, ctIPd must know to which server it should connect. There are several servers worldwide, and ctIPd includes a built-in failover mechanism to handle cases of connectivity failure so you do not need to provision any special means to handle connectivity failures.

To do this, specify the DNS string that you have received from CYREN in the `ServerAddress=` setting in ctipd.conf file. The value contains a `%d` sequence within the DNS string. The DNS string is translated to a Datacenter identifier.

If ctIPd experiences any connectivity problems, it will automatically try to connect to an alternate Datacenter by replacing the %d with a different identifier. It is imperative that you use the exact DNS string as received from CYREN without making any modifications to it. If it is changed, either ctIPd will be unable to receive service, or the built-in failover mechanism will not work. For more information on the server address you should receive from CYREN, refer to the *ctIPd Implementation Guidelines*.

Protocol Issues

ctIPd can communicate over the following protocols:

- HTTP
- UDP
- RBL/RBL+

By default, `ctIPd` is configured to allow communication with querying devices over HTTP and UDP protocols and to decline communication over RBL/RBL+ protocol.

If you wish to communicate with ctIPd over RBL/RBL+ protocol, you should first enable this option in the [RBL] section of the ctipd.conf file and make sure to specify the domain name of the ctIPd host as described in the *ctIPd Integration Manual*. Some OEM partners choose to test and evaluate ctIPd over RBL/RBL+ even if later, during standard operation, they expect to be using it over HTTP or UDP.

For more information on the protocols that are used and how they are configured, refer to the *ctIPd Integration Manual*.

Logging Method

ctIPd includes three scripts to generate reports on the daemon's activity and performance. These reports are helpful during the evaluation phase as well. The reports query ctIPd's internal logfiles and generate a predefined selection of data. The data is sent to stdout and you may redirect it as a raw input data to a statistical analysis application, Excel worksheet, or database.

By default, the LogMethod option in the configuration file is set to 0, which means that no logfiles are created and therefore no reports can be generated. This functionality is disabled initially in order to allow you to set up the necessary settings for the storage before ctIPd begins storing logfiles to your disk. It is recommended that you allocate some disk space for these logfiles and change `LogMethod=1` in the configuration file during the testing phase. Logging and the reports that can be generated are detailed in the *ctIPd Reporting Guidelines* document.

Proxy Settings

If you connect to the Internet through a proxy server, the ProxySettings options in the [IPREP] section of the configuration file should be assigned with appropriate values. For more information on the proxy options available in ctIPd, refer to the *ctIPd Integration Manual*.

Testing Options

Once you have successfully deployed ctIPd, it is recommended that you test ctIPd at two levels to confirm that it is correctly receiving and responding to queries sent by your querying device and that it is correctly classifying these queries.

- The first level is considered Acceptance testing and can be accomplished using the IP addresses detailed in the CYREN Predefined Fixed IP Addresses section. This method uses predefined data and then matches the results against known classifications and expected results.
- The second level is designed more for evaluation purposes and involves using ctIPd to process a large amount of queries to evaluate performance. This can be accomplished either by redirecting a predefined feed of IP addresses with known results or redirecting a live feed of IP addresses from your MTA. You can "fork" traffic without impacting your ongoing messaging network and then analyze the results using ctIPd's built-in reports.

Acceptance Testing

To properly test ctIPd, CYREN has provided several Perl scripts which receive a list of IP addresses in a command line and forward them to ctIPd for classification. This process includes the following:

1. You can either enter a parameter in the command line, or read the IP addresses from STDIN until EOF.
2. You must specify the hostname and port where ctIPd runs. By default, this is localhost and port 8080 for HTTP and 5678 for UDP.

CYREN Predefined Fixed IP Addresses

For effective testing, CYREN predefined the following IP addresses with fixed values to be returned in responses to `classifyip` requests:

Test IP	IPClass	Risk	Volume	SpamR	BulkR	TTL	MaxHits
216.163.176.201	G1	0	0,5,4	0,0	3	1h	Null
216.163.176.202	G2	100	0,5,4	92,90	0	2h	Null
Private IP Ranges	G3	0	1,0,0	Null	Null	Null	Null
	For more information, see Example of Private IP Addresses.						
216.163.176.211	T1	38	0,5,1	0,35	5	Null	16
216.163.176.212	T2	56	0,1,2	55,59	0	Null	0
216.163.176.213	T3	73	0,3,3	100,42	57	Null	4

Test IP	IPClass	Risk	Volume	SpamR	BulkR	TTL	MaxHits
216.163.176.214	T4	87	300,2,1	89,84	0	Null	8
216.163.176.215	T5	95	-31,4,5	93,97	1	Null	16
216.163.176.221	R1	3	0,7,0	0,3	0	10min	Null
216.163.176.222	R2	7	0,6,2	0,6	0	30min	Null
216.163.176.223	R3	15	-35,6,6	0,12	67	30min	Null
216.163.176.224	R4	29	-91,6,6	56,0	99	30min	Null
216.163.176.225	R5	51	0,7,6	63,1	94	30min	Null
216.163.176.226	R6	68	62,6,5	90,49	20	30min	Null
216.163.176.227	R7	72	0,7,8	59,74	9	30min	Null
216.163.176.228	R8	88	40,8,5	94,81	3	30min	Null
216.163.176.229	R9	95	0,7,5	0,97	0	1h	Null

After running these tests, you may also add `x-ctch-cache-only` to the next `classifyip` request to receive zero-latency response. Additionally, you may want to simulate one or more cases of returned errors by ctIPd. To do this you can review the list of returned errors in the protocol and generate queries that will result in having `x-ctch-request-status` return value different than '0'. For example, you may disrupt the query with bad format or missing data or use an invalid IP in the request, etc.

Example of Private IP Addresses

```
From          To              Representation
----------    --------------  ---------------
10.0.0.0      10.255.255.255  10/8
172.16.0.0    172.31.255.255  172.16/12
192.168.0.0   192.168.255.255 192.168/16
127.0.0.0     127.0.0.255     127/8
```

RBL/RBL+ Testing

For performing the Acceptance Testing for querying IPs over RBL/RBL+, the query must specify an IP address and the specific zone, as detailed in the *ctIPd Integration Manual*. The response will be in the form of an IP address based on the information presented in the table. For each IP address queried, the sample IP address (from the above table) will be correlated to an IP class and the appropriate response will be forwarded back for the specified zone.

The response over RBL/RBL+ contains Header, Question, and Answer sections. The following zones are available:

1. std.rbl.<domain_name> - keeps information about backlisted and 'grey' sources.
2. black.rbl.<domain_name> - keeps information about blacklisted-only sources.
3. grey.rbl.<domain_name> - keeps information about 'grey'-only sources

Note: *<domain_name> represents the specific domain name that is used for the machine that hosts ctIPd and it is different for every implementation. This value is configured in ctipd.conf within the [RBL] section.*

The RBL+ zone named plus.rbl.<domain_name> also keeps information about blacklisted and 'grey' sources and is used for responding with 127.0.0.2 for blacklisted sources and 127.0.0.3 for 'grey' sources in a single response. This is different than the RBL zone, std.rbl.<domain_name> that responds with 127.0.0.2 for sources that are either blacklisted or 'grey' sources.

For example, the following query could be sent from the querying device:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27762
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
; 216.163.176.202.std.rbl.mycompany.com.    IN   A
```

This query is asking ctIPd to check a specific IP address to see if it is listed in either the black or grey zones. ctIPd will be expected to return the following in the answer section of the response:

```
;; ANSWER SECTION:
216.163.176.202.std.rbl.mycompany.com. 0 IN  A    127.0.0.2
```

This response indicates that a match was indeed found and the querying device would be expected to reject the SMTP connection.

HTTP/UDP Testing

For evaluating over HTTP or UDP, the following sample scripts are available:

For HTTP: scanip_http.pl

For UDP: scanip_udp.pl

Usage is the same for both sample scripts:

```
./<script's name> [OPTIONS][IP(s)]
```

Command line switches are as follows:

OPTIONS

- `--host` Define the server host. Default is 127.0.0.1
- `--port` Define the server port. Default is '8080' for HTTP and '5678' for UDP.
- `--cache` Dend a cache-only request. Default '0'.
- `--help` Display the help message.

For input, you may feed the sample scripts with one or more IP(s) from `stdin` or a file.

Evaluating Test Results

After you have completed the Acceptance testing, it is beneficial to evaluate ctIPd performance and actions by passing large volumes of queries from the querying device to ctIPd. This can be accomplished by redirecting a predefined feed of IP addresses with known results or by redirecting a live feed of IP addresses.

You can then generate some or all of ctIPd's built-in reporting scripts to evaluate ctIPd responses based on specific transactions or recommended actions, or more wide-ranging statistics on a daily or general basis.

ctIPd Reports

The following ctIPd reports are available:

- *get_tran:* output one or more transactions from the internal logfile for predefined values such as the transaction ID (ctid) or IP address (or a series of addresses). This report is designed mainly for use by technical support to handle incidents and diagnostics.
- *get_action:* display all the transactions for one or more predefined IP addresses filtered by call-to-action (accept, tempfail, permfail). This report can be used to research and analyze how ctIPd operates or the type of attacks that impact the organization and a behavioral study of attackers.
- *get_stats:* generate statistics with a daily breakdown or for an entire period. This report can be used to research and analyze how ctIPd operates or the type of attacks that impact the organization and a behavioral study of attackers.

For a detailed explanation of each of the above reports, refer to the *ctIPd Reports* document.

Checking IP Reputation Data

Although ctIPd delivers a very high accuracy in determining the reputation of sources in real-time, there may be instances where IP reputation data users may occasionally feel that an IP sender should have been classified differently. To enable CYREN to fix any mistakes in reputation, CYREN has implemented a reporting system to enable OEM partners to report any reputation errors. This is not necessary if you are testing ctIPd with predefined messages. However, if you are testing ctIPd with a live feed, you may be able to improve overall performance even more if you report any errors.

You can use CYREN's web-based IP reputation reporting system by visiting: http://www.CYREN.com/Site/Resources/Check_IP_Reputation.asp. The report is posted to the CYREN technical support for immediate processing and handling. Although no response is sent directly to the user, those who report an IP reputation error can recheck the status of their IP address using the Check IP Reputation tool on the CYREN website to confirm that the problem has been fixed.

Alternatively, if you prefer that your customers connect to your website and not to the CYREN website to check IP reputation mistakes, you have the option of hosting this iFrame tool on your website.

If you choose this option, it is highly recommended that you add your ClientID within the request that is sent to CYREN. For more information, see the *ctIPd Implementation Guidelines*.

Note:	*The ClientID is provided to you by a CYREN representative along with the DNS server string and license key code.*

Additional ctIPd Documentation

The following documents can assist you in understanding, implementing and integrating ctIPd.

- *ctIPd Getting Started*
- *ctIPd Product Description*
- *ctIPd Implementation Guidelines*
- *ctIPd Integration Manual*
- *ctIPd Logs and Reports*

Contacts

Any technical questions you or your developers have about using the ctIPd 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

ctasd is a licensed SDK product featuring patented technology. CYREN's patented solution is protected by U.S. patent #6,330,590.