CYREN

ctIPd™ Product Description

CYREN GlobalView™ Mail Reputation services are used primarily to weed out spam messages and email-borne malware at the entry point before these messages enter the customer's messaging network, thereby relieving the need for resource-consuming downstream filtering. This is accomplished by applying the most up-to-date IP reputation data to the sender IP, before the SMTP connection is accepted.

By applying GlobalView Mail Reputation services to the senders' IP addresses before or during the SMTP connection and before their messages enter the messaging network, ctIPd delivers cost-effective benefits such as the following:

- Reducing IT resources such as server count, CPU load, storage, etc.
- Eliminating multiple security risks
- Reducing the level of false positives
- Minimizing the cost of downstream filtering
- Lowering the overall bandwidth consumption
- Optimizing IT labor required to manage the overall messaging process

Additionally, CYREN GlobalView Mail Reputation services are used as part of an overall strategy to optimize network accessibility so that the network's messaging processes are efficient and focused on allowing legitimate sources full and uninterrupted access. At the same time, the CYREN GlobalView Mail Reputation services also make access for unauthorized sources with bad reputations attempting to abuse the network more difficult to achieve.

Many public services nowadays already deliver free information about blacklisted sources; typically, these lists are static with limited commitment for accuracy by the owners. Other commercial services also enable setting central as well as personal policies for whitelisted sources during the SMTP session.

However, these solutions are not designed to handle the vast 'grey' area of sources for which little or no information is readily available. Included in this group, for example, are millions of machines hijacked on a daily basis and forced into botnets and armies of zombies discrediting their reputation dynamically. Many of these bots are detected at a later time and are removed and thus the reputation of the once-infected machines is improved.

CYREN analyzes hundreds of millions of messages every day. Included in this analysis is a process whereby CYREN dynamically and in real-time classifies and reclassifies the reputation of each source IP with a series of meaningful and measurable values. These values are constantly updated to include the most up-to-date information and reflect even the slightest change in credibility.

The CYREN GlobalView Mail Reputation daemon (ctIPd™) is an embedded reputation engine with a small footprint. It is responsible for maintaining communication with the CYREN Datacenter. ctIPd delivers reputation data to messaging, security and networking devices, providing an added layer of protection while saving valuable resources by enabling the messaging network to analyze and process requests before messages reach the network. These querying devices post queries to ctIPd over HTTP, UDP, or RBL/RBL+ protocol requesting reputation data on source IP addresses attempting to establish SMTP sessions for sending messages to recipients.

ctIPd analyzes all available data and provides a suggested call-to-action that is relayed back to the querying device. In response to ctIPd's call-to-action, the querying device will accept, tempfail, or permfail the connection from a sending SMTP source.

Alternatively, a non-CYREN flow control or connection management application on the client-side can be configured to receive raw reputation data from ctIPd and then weigh the responses and make its own determination for the appropriate actions to implement.

By applying ctIPd-recommended actions based on real-time, precise information about globally monitored behavior of source IP addresses, the customer is able to throttle unknown and suspected sources while freeing its bandwidth more efficiently to legitimate, non-spam related messages.

The purpose of this document is to describe CYREN ctIPd architecture, deployment scenarios, the different ways that ctIPd may be used to deliver accurate reputation information, and its overall system requirements.

The CYREN GlobalView Mail Reputation solution includes the following components:

- Querying device
- ctIPd daemon
- ctIPd protocol
- CYREN Datacenter

Querying Device

For the purposes of this document, the term "querying device" is used as a generic term for mail transfer agents (MTA), security appliances, networking devices, or any device that is capable of receiving email messages or monitoring SMTP traffic and generating a query to ctIPd over HTTP, UDP, or RBL/RBL+ interfaces. Once a response from ctIPd is received, the querying device is responsible for applying connection management decision and flow control actions based on ctIPd's response.

ctIPd

The CYREN IP Reputation embedded daemon (ctIPd) receives and processes incoming requests from querying devices to determining the reputation of specific source IP and quickly responding to the querying devices with details on several key data types along with recommended action. Typically, ctIPd is deployed on-site in order to guarantee high performance and availability to local querying devices.

ctIPd Protocol

In order to enable communication between a querying device and ctIPd and simplify the integration process for its OEM partners, CYREN has developed a simple communication protocol. This protocol enables OEM partners to communicate with ctIPd and thereby to provide Mail reputation services to their users. Communication between ctIPd and the querying device can be accomplished over HTTP, UDP. Alternatively, interfacing over RBL/RBL+ protocols is supported as well.

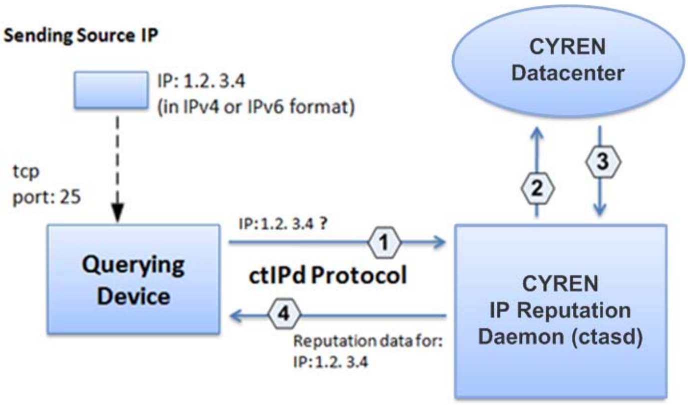
CYREN Datacenter

The CYREN Datacenter monitors global email traffic in real-time (24*7*365) from various sources on an ongoing basis and maintains a vast database of GlobalView Mail reputation classifications that are determined based on numerous dynamically changing parameters.

System Architecture and Data Flow

Although the data flow of ctIPd can vary depending on configuration settings and deployment scenarios, a typical data flow is detailed below:

1. A source IP attempts to send messages to recipients. Typically, this would initiate an SMTP connection to transfer the data. Before any data is transferred between the sending IP and the mail server, the querying device uses the CYREN ctIPd protocol to generate a query to ctIPd about the reputation of the sending IP.
2. ctIPd prepares and forwards a query to a CYREN Datacenter to retrieve the most up-to-date information based on global and dynamic behavior of the source IP.
3. The CYREN Datacenter responds to ctIPd with current information regarding the sender IP.
4. ctIPd collects IP reputation data along with some cumulated stats about local exposure to the same sender.
5. After analyzing all available data and formulating a call-to-action (accept, tempfail, permfail), ctIPd reformats the response into the appropriate protocol and sends the response back to the querying device over the same protocol used by the initial query.



The querying device, upon receiving the response from ctIPd, implements ctIPd's recommended call-to-action. Alternatively, ctIPd can be configured to forward raw IP reputation data to the querying device with or without the call-to-action.

The querying device can also separately initiate passing a series of IP addresses to ctIPd that are already known to it as being 'good' and 'bad' sources as well as passing the decision that it has made on the queried IP after the response from ctIPd was received. This information may have been gained by another querying device, policy, or reputation service. When passed to CYREN, it can become part of the database of IP reputation classifications. This will assist ctIPd in quickly and correctly responding to future queries about these sources.

ctIPd Response Options

Once ctIPd has analyzed available data, it will return one of the following call-to-action responses to the querying device:

Response	Explanation
accept	The IP address is not currently recognized as a “bad” source and therefore it is recommended that the pending SMTP session be accepted.
tempfail	Enough data has been collected to suggest that the IP source may be a “bad” source but the data is not conclusive. It is recommended that the querying device will tempfail the connection allowing the source to reestablish the connection at a later time. All legitimate sources are equipped with a resending mechanism in response to tempfail response while only few bot applications are designed with such capabilities.
permfail	Enough data has been collected to determine that the IP source is sending malicious content (spam, virus, etc.) and therefore it is recommended that the SMTP session be rejected.

To offer the maximum flexibility to the OEM partner, ctIPd’s response to each query can be configured in a variety of ways, from having ctIPd forward all of the available raw data with no recommended action to having ctIPd forward only the recommended action. For example:

- Some OEM partners use only the IP class and Risk Level, while other OEM partners use all of the reputation data to determine which decisions and/or actions their flow control application will apply to incoming traffic from a sender IP.
- Others use only the Action contained in ctIPd response without consulting additional reputation sources.
- Still other OEM partners choose to incorporate additional response data types in the configuration or policy options.
- Some OEM partners only want to receive the recommended action, trusting CYREN’s extensive data-collecting mechanisms to correctly and adequately provide IP reputation data.

ctIPd’s comprehensive response syntax offers maximum flexibility and ease of integration by enabling each OEM partner to make use of any part of the Mail reputation response to determine an appropriate action regarding sender IP reputations.

Response Data Types

Each time ctIPd receives a `classifyip` request from the querying device over HTTP or UDP, it returns a response. By default, the response includes the following:

- IP range
- A call-to-action
- A RefID (the contents of which may vary depending on enabled actions within the configuration file).

Alternatively, you have the option to have ctIPd include raw data information in the body of the response, including IP class data. For more information on other raw data, see the *ctIPd Integration Manual*.

IP Class Groups

By default, the IP class data type is only included in the response if you enable the `SendRawData` parameter in the configuration file. The IP class represents a composite reputation value assigned by CYREN. There are three groups, each represented by a letter (R, T, or G) and a number. The number represents the level of risk.

- Groups R and T represent the volume received in a 24-hour period.
- Group G, the **Known Reputation** group, represents sources with fixed decisions, not based on their monitored volume. These include blacklisted, whitelisted and private IP sources.

A variety of elements are used to determine the risk value. By combining the volume and risk, CYREN has determined set IP classes that fall into three groups:

- High Volume
- Transitory or Low Volume
- Known Reputation

Group	Explanation
Rx: R1..R9	Represents sources with substantial volume history. For example, R1 being a source that was monitored over time with high volume and low risk and R9 a source with high volume and high risk.
Tx: T1..T5	Represents sources with transitory volume or no volume history. For example, T1 being a source with low transitory volume and low risk and T5 a source with low transitory volume and high risk.
Gx: G1..G3	Represents sources for which there are fixed decisions and regardless of their monitored volume. In this group, G1 are all whitelisted sources, G2 are all blacklisted sources, and G3 are all private IP sources.

To requests over the RBL/RBL+ interface, the response from ctIPd specifies the call-to-action based on the queried zone as a typical 127.0.0.2 or 127.0.03 response.

ctIPd Deployment Options

ctIPd can integrate with a wide variety of applications and devices to enable IP reputation services. The deployment options are adaptable to the individual requirements and infrastructure of the CYREN OEM partner and its customers.

Following is a partial list of ways in which ctIPd can be deployed:

- ctIPd can be integrated with the OEM MTA and/or flow control application on the same box, or ctIPd can be deployed on a separate box.
- ctIPd can be deployed using CYREN's Decision Manager Module to determine appropriate actions, or integrated with an existing flow control application for analysis of the raw reputation data in ctIPd's response.
- A single ctIPd can be used to serve one or more querying devices, simultaneously.
- Multiple ctIPd can serve one or more querying devices.
- One or more ctIPd daemons can run on the same machine.

ctIPd is typically deployed on the customer's premises, thus requiring no authentication of the querying devices. Nonetheless, ctIPd requires authentication of communication between ctIPd itself and the CYREN Datacenter on behalf of the customer.

IPRep Supported Protocols

CYREN has developed a simple protocol to enable communication between the querying device and ctIPd. Using a pre-determined syntax for the envelope and data contained in a query, the querying device sends requests to ctIPd over HTTP, UDP, or RBL/RBL+ protocol. Once processed, ctIPd responds to the request (or returns an error message, if the request could not be processed). The protocol structure over HTTP/UDP is extensible, meaning that the order of the MIME-based headers is not mandatory and not all headers are required to be included in all responses.

A typical communication session would begin with the querying device initiating a request to ctIPd asking for reputation data. The communication would include some or all of the following:

- The querying device sends a request for reputation data about a single IP address.
- ctIPd receives the request and sends back a response. This response contains various values related to the IP range to which the queried IP belongs. It may contain raw data used to make a recommendation, or call-to-action, or it might contain both the raw data and a recommendation.
- Once the response is received, the querying device applies an appropriate flow control decision to the session based on the information contained in the response. A non-CYREN flow control or connection management application may weight responses from multiple processes before applying its final decision.

ctIPd Reports

ctIPd includes pre-defined reports that detail the daemon’s activities and performance based on time, actions, or a specific IP address or group of addresses. The command line reports are initiated by scripts to query ctIPd’s 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 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.

SNMP Counters

ctIPd maintains a series of SNMP agents to monitor the daemon’s performance and to log its activities. The SNMP agents maintain counters on key performance data, including the following:

- Total number of requests currently in progress.
- Total number of requests waiting in the queue to be processed.
- Total wait time to date for all requests.
- Total number of classifyip requests that have been processed by ctIPd (over a specific protocol or over all protocols combined).
- Total number of tempfail responses.
- Total number of accept responses.
- Total number of permfail responses.
- Total number of records currently in the local Decision Manager cache.

- Total amount of processing time required to date for all requests.
- Total number of reportip requests that have been sent to ctIPd.
- Total number of errors that occurred as a result of classifyip requests to the ctIPd.
- Total number of errors occurred as a result of reportip requests to the ctIPd.
- Total number of records currently in the cache.
- Total number of times the local cache was able to provide IP reputation.
- Total number of times the local cache was unable to provide IP reputation, triggering a query to the CYREN Datacenter.

Supported Platforms

ctIPd is compiled for the following platforms:

- Windows 32 Bit
- Linux
- FreeBSD
- Solaris 9/10 32bit over SPARC
- Solaris 9/10 32bit over x86

The ctIPd package includes all system libraries and dependencies it requires.

ctIPd Deployment Requirements

Following is a list of recommended hardware requirements:

- Single CPU, 2.8 GHz
- 1 GB RAM
- 80 MB free disk space
- 100 Mbps Network interface

ctIPd Package Contents

The ctIPd package contains the following:

- ctIPd daemon and associated binary
- ctIPd default Decision Manager module
- ctIPd documentation
- Sample files for quick evaluation and testing

Contacts

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

About CYREN

CYREN^{TM} 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

CTT40-400-911-081-R1