ctIPd™ Implementation Guidelines

Checklist and Recommendations

CYREN GlobalView™ Mail Reputation Service, provided by the CYREN IP Reputation daemon (ctIPd) is 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. ctIPd supports both IPv4 and IPv6 formatted IP addresses (though it does not support IP ranges in IPv6).

This document presents a variety of ways in which ctIPd can be implemented within the organization, according to the specific needs and preferences of each application.

It is designed for Service Providers, OEM partners, 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.

This document is divided into the following sections:

- Technical Specifications
- Deployment Options
- Failover Considerations
- Configuration File Options and Guidelines
- Explanation of the internal logic used to determine calls-to-action
- Logging and Reporting Options
- Updates and Versioning
- RefID and ctid Reference Values
- Checking IP Reputation Data
- Reporting Cases of Reputation Mistakes

Technical Specifications

Supported Platforms

ctIPd is compiled for generic support of the various distributions and versions of the following platforms:

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

Package Contents

The ctIPd package includes all system libraries with which it was compiled on non-Windows platforms and with all the dependencies it requires. It is compatible with all Linux or FreeBSD versions. It does not necessitate any special flavor/version-dependent requirements and can run on the same host alongside other applications that were compiled differently.

Recommended Hardware

Following is a list of the minimum recommended hardware configuration:

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

Deployment Options

Typically, ctIPd is deployed on the customer's premises. In this deployment scenario, no authentication is required between ctIPd and the querying devices. However, authentication is still required for communication between ctIPd and the CYREN Datacenter.

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

Following is a list of typical scenarios in which ctIPd can be deployed:

- ctIPd can be integrated with the querying device (such as the MTA, UTM appliance, other security device) on the same box or on a separate box.
- A single ctIPd can be used to serve one or more querying devices, simultaneously.
- Multiple ctIPd can serve one or more querying devices.

Running Multiple ctIPd Daemons

In general, it is recommended that you deploy at least two ctIPd units for redundancy and failover. Additional units may be recommended for load-balancing and failover depending on a variety of factors, including:

- The number of MTA systems – if ctIPd is deployed on the same box as the security device and each MTA uses a dedicated security device. In this scenario, a single ctIPd unit is needed for each security device. Alternatively, if the ctIPd unit is deployed outside the security device, than it can serve multiple security devices and MTA systems.
- Geographic conditions – may require multiple ctIPd daemons to be deployed in various locations for the same organization or in different messaging access points of the global network of some organizations.

Failover Considerations

To handle failover to multiple ctIPd units when one of the units is unavailable, see the guidelines above.

To handle failover to multiple CYREN Datacenters, the ctIPd daemon contains a built-in failover mechanism. The existence of this mechanism relieves the end-customer from the need to worry about continuity of service. Successful operation of this mechanism is dependent on the DNS string that is defined in the configuration file as the `ServerAddress=` parameter. For more information about this parameter, see later sections in this document.

Configuration File Options and Guidelines

License Key Customization

The CYREN Datacenter is responsible for maintaining a vast repository of threat-related classifications and categorizations related to email and web security. ctipd communicates with the Datacenter to receive IP reputation data. Communication is authenticated based on a license key, a mandatory value that is supplied as a parameter in the Connection String, and consists of the following:

- **CYREN token:** 20-character unique identifier provided by CYREN to identify the OEM partner and Service Partners
- **OEM token:** A unique identifier (up to 35 alphanumeric characters) provided by the OEM partner and Service Partners

The OEM/Service Partner identifier should distinguish between each user, device, or installation. In cases where more than one CYREN product or service is installed on the same device, a unique token should be created per instance. The token should be unique for the lifetime of the host application and should not be changed so that the same OEM/Service Partner token is used each time the application is initiated. It can be based on hardware or software-specific data. CYREN needs this full license key format to offer the highest level of customer support and service.

The format for this concatenated parameter uses a colon delimiter, as follows:

```
LicenseKey=<CYREN token>:<unique OEM token>
```

Example: `LicenseKey=0001K032B1010W167E2B:12345-1234A-55555`

DNS Server

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.

Protocols

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*.

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

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*.

Decision Manager Logic

By default, ctIPd returns a recommended call-to-action for each query received. The action could include a recommendation to accept a pending SMTP connection that was initiated by the queried source IP, temporarily reject the SMTP connection (tempfail), or permanently refuse the connection (permfail).

ctIPd returns these recommendations based on computed reputation data available at the time of each query. The reputation is computed from a variety of dynamically modified values, including the IP Class that is provisioned by the CYREN Datacenter, the timing and number of requests about the source IP received within a specified period of time (the level of local exposure to the source IP), and more.

IP class is a critical element in the decision process for determining the recommended call-to-action. In most cases, queries about IP addresses with good reputation will be accepted and queries about sources with notorious reputation will be rejected, automatically. Queries about sources with other reputation levels will be responded with varied recommended calls-to-action depending on the intensity of the source attempts to connect. This is managed by controlling and limiting the rate at which these attempts to connect are accepted (i.e., throttling).

Understanding Throttling

Typically, MTAs that are dynamically detected while sending a mixture of harmless and legitimate messages along with Spam or malicious messages, are considered suspicious. Some suspicious sources send Spam messages only occasionally and normally they behave like regular good sources. This means that most but not all sent messages should be accepted. Other suspicious sources send mostly Spam and malicious messages and should be blocked to avoid infiltration of unwanted and sometimes malicious content.

A special case is a source that is unknown to CYREN at the time of the query. The source is considered suspicious until proven “innocent” some minutes later. This is because CYREN already has classified nearly all the legitimate sending MTAs and the Datacenter is designed to quickly update its definition of new good sources.

Because of these constant updates, chances are very small that a new unknown source is not a recently-hijacked host used to send Spam and malicious messages. This assumption is backed up with documented evidence that shows that nearly 90% of the messages on the Internet are Spam or malicious and that over 85% of these emails are sent and distributed by “zombie” hosts.

Therefore, an unknown source is considered a “lightly” suspicious source until its true reputation is computed. Typically, this process takes a very short period of time until the “new” IP becomes known as either a zombie/Spammer or a legitimate source. If it turns out to be a legitimate source, than it will always be accepted. Otherwise, if it turns out to be a spamming source, than its suspicious level will be increased and accordingly, its future attempts to establish a connection will be rejected.

Throttling was designed to handle suspected sources by limiting the rate at which their attempts to connect are accepted. Each source is limited differently according to its level of suspiciousness. This level is a combination of the IP Class of the source, which already blends a handful of backend calculations about the source and the intensity of connections. Throttling means that for a predefined time-based window some messages are accepted and others are rejected with a tempfail response. For example, a throttling logic may dictate accepting only 1 message every 15 minutes.

According to ctIPd’s internal logic, messages from legitimate sources are accepted when they arrive because the normal behavior of correspondence might include several messages that are exchanged sporadically throughout the day and in low to medium intensity (even if multiple contacts at both organizations converse, separately). However, with the exception of perhaps 1 message every 15 minutes in this example, all the messages sent from a bad source will be rejected. Normal behavior for such bad sources results in a spray of the same messages sent to different recipients in the organization at a high rate. The throttling logic is set differently for every IP Class of the source.

Understanding CYREN Decision Manager’s Logic

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. Otherwise, a default template is used and typically it would accommodate most customers’ needs.

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

The values and logic displayed in the following tables were carefully developed by CYREN based on years of experience. The purpose of these templates is to determine and apply the best results for when both good and bad sources are trying to establish SMTP connections. These templates outline the predefined logic for recommending calls-to-action per template.

Small Template

The *Small* template is intended for deployments processing an average of less than 3,000 SMTP connections per day (per ctIPd unit).

IP Class	First Action	Second Action
T1	Accept	No further action is necessary
T2	Accept	No further action is necessary
T3	Tempfail during first 14min	Accept 1 connection and tempfail all others in 15 minute cycles
T4	Tempfail during first 14 minutes	Accept 1 connection and tempfail all others in 15 minute cycles
T5	Tempfail during first 14min	Accept 1 connection and tempfail all others in 30-minute cycles
R1...R6	Accept	No further action is necessary
R7	Tempfail during first 14min	Accept 1 connection and tempfail all others in 15 minute cycles
R8	Tempfail during first 14min	Accept 1 connection and tempfail all others in 15 minute cycles
R9	Tempfail during first 14min	Accept 1 connection and tempfail all others in 30-minute cycles
G1	Accept	No further action is necessary
G2	Permfail	No further action is necessary
G3	Accept	No further action is necessary

Medium Template

The *Medium* template is intended for deployments processing an average of 3,000 – 300,000 SMTP connections per day (per ctIPd unit). This is the default template applied to most deployments.

IP Class	First Action	Second Action
T1	Accept	No further action is necessary
T2	Accept	No further action is necessary
T3	Tempfail during first 14min	Accept 2 connections and tempfail all others in 15 minute cycles
T4	Tempfail during first 14min	Accept 1 connection and tempfail all others in 15 minute cycles
T5	Tempfail during first 14min	Accept 1 connection and tempfail all others in 30 minute cycles
R1...R6	Accept	No further action is necessary
R7	Tempfail during first 14min	Accept 2 connections and tempfail all others in 15 minute cycles
R8	Tempfail during first 14min	Accept 1 connection and tempfail all others in 15 minute cycles
R9	Tempfail during first 14min	Accept 1 connection and tempfail all others in 30 minute cycles
G1	Accept	No further action is necessary
G2	Permfail	No further action is necessary
G3	Accept	No further action is necessary

Large Template

The *Large* template is intended for deployments processing over 300,000 SMTP connections per day (per ctIPd unit).

IP Class	First Action	Second Action
T1	Accept	No further action is necessary
T2	Accept	No further action is necessary
T3	Tempfail during first 14min	Accept 3 connections and tempfail all others in 15-minute cycles

IP Class	First Action	Second Action
T4	Tempfail during first 14min	Accept 2 connections and tempfail all others in 15-minute cycles
T5	Tempfail during first 14min	Accept 1 connection and tempfail all others in 30-minute cycles
R1…R6	Accept	No further action is necessary
R7	Tempfail during first 14min	Accept 3 connections and tempfail all others in 15-minute cycles
R8	Tempfail during first 14min	Accept 2 connections and tempfail all others in 15-minute cycles
R9	tempfail during first 14min	accept 1 connection and tempfail all others in 30-minute cycles
G1	Accept	No further action is necessary
G2	Permfail	No further action is necessary
G3	Accept	No further action is necessary

Disabling the Decision Manager Functionality

By default, the Decision Manager functionality is enabled and ctIPd will return a call-to-action for every received query. If you wish to disable this functionality, you should disable this functionality in the [DecisionManager] section in the ctipd.conf configuration file by changing the `Enabled` value to `no` and enabling sending the raw reputation data in the response to classifyip requests.

To enable sending the raw reputation data, change the `SendRawData` value to `yes` in the [IPRep] section

Note: *If you change the configuration file while ctIPd is operating, you must restart ctIPd in order to have these changes take effect. ctIPd only checks the configuration file at startup and does not update the current configuration parameters until the next startup.*

Logging and Reporting Options

ctIPd includes three scripts to generate a variety of reports on the daemon's activity and performance. 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. The logfiles are used internally by ctIPd and therefore, are not described. Furthermore, the structure of these logfiles is subjected to frequent changes by CYREN without prior notice to its OEM partners.

Logging Options

If enabled, there are two logging options available in ctIPd. 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 in order to let your users extract the relevant reports from time to time.

The two logging options that can be defined in the ctipd.conf file:

LogMethod	Explanation
1	ctIPd will locally log every transaction to internal logfile that may be used by the reporting scripts to generate various reports. This is the recommended method for logging.
2	ctIPd will include all the relevant transaction data in the response to `classifyip` requests and the OEM application is responsible for parsing the data and using it in non-CYREN reporting tools.

Reporting Options

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.

Updates and Versioning

CYREN distributes ongoing updates of ctIPd as needed throughout the year and, on occasion and as development cycles require, full version upgrades. For new versions OEM partners are notified in advance to download the latest build from the CYREN FTP server. These builds are tested extensively in-house before being released. Once released, they can be used to transparently auto-upgrade the existing daemon version currently at your customers' sites.

When CYREN creates a version that requires you to further integrate with your product beyond the transparent auto-update, CYREN announces this update months in advance to enable you to synchronize with your internal schedule of releases.

Note: *In order to subscribe to receive these ongoing notifications about updates, contact Technical Support at oem.support@commtouch.com.*

RefID and ctid Reference Values

To track transactions, CYREN includes reference values The `RefID` is a reference ID record that will be used by CYREN to diagnose various support issues, per-transaction. It is recommended that you keep this RefID in case you need to trace back to determine why ctIPd returned any particular response. The syntax of the RefID changes according to the options that you have enabled within the ctIPd configuration file.

Note: *Without this key, CYREN is unable to retroactively determine the reason why a query was returned with any specific set of data values.*

At a minimum, the RefID will contain the transaction number (`ctid`) and the call-to-action for the query. If enabled, it may also contain details of the raw reputation data and logging. It is recommended that you keep these values (both RefID and ctid) in case you need to trace back to determine why ctIPd returned any particular response.

These values should be available when contacting CYREN. If they are not saved, CYREN cannot retroactively trace back the information in the transaction to determine why a recommended call-to-action was made.

The ctid will appear in the RefID record of every response to classifyip request over HTTP and UDP protocols. In the case of RBL/RBL+, this key is returned only when a DNS TXT query is made. The key also appears in the logfile when LogMethod is set to 1.

Checking IP Reputation Data

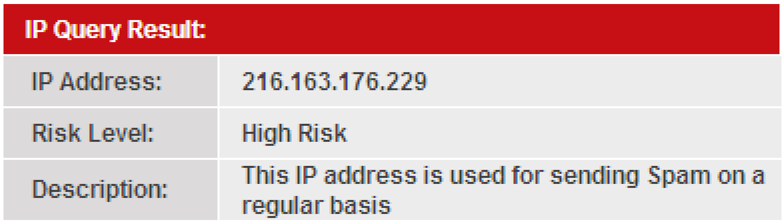
The CYREN website includes a free web-based tool that enables you to check the latest reputation data available for an IP address. You should encourage your customers to use this tool. The tool can be accessed at:

http://www.commtouch.com/Site/Resources/Check_IP_Reputation.asp

To use the Check IP Reputation application:

1. Enter an IP address in the IP Address field.
2. Enter the captcha verification code.
3. Click **Show Current Reputation**.

The tool will submit a request to a ctIPd unit at CYREN and display the results. The results, including the queried IP address, the risk level, and a description, will be displayed in the browser window. The Risk Level is translated to plain language that any CYREN and non-CYREN user of this web tool can understand.



IP Query Result:	
IP Address:	216.163.176.229
Risk Level:	High Risk
Description:	This IP address is used for sending Spam on a regular basis

Reporting Cases of Reputation Mistakes

Although ctIPd delivers a very high accuracy in determining the reputation of sources in real-time, users may occasionally feel that an IP sender should have been classified differently. By reporting any cases of such reputation mistake to CYREN, you can improve the overall performance even further.

To report cases of reputation errors:

1. Open a browser and navigate to: http://www.commtouch.com/Site/Resources/Check_IP_Reputation.asp
2. Click the link **Report a Mistakenly Blocked IP Address**. A form appears with the following fields:
   - First name *
   - Last name *
   - Company name
   - Job Title
   - Email *
   - Phone
   - IP Address *
   - Description

   - Recipients List
   - Contents of non-delivery report

Note: *The fields indicated with an asterisk (*) are mandatory.*

3. Enter the verification text in the appropriate field and click **Submit**.

The report is posted to the CYREN technical support for immediate processing and handling. Although no response is sent, 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 and/or report reputation mistakes, you have the option of hosting this 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. When this value is returned to CYREN, CYREN will be able to identify that the query relates to one of your distributed license keys and allow technical support to better investigate the problem based on customized settings that may have been applied to your keys.

For example, CYREN may need to confirm that the correct Decision Manager logic is being applied to your organization. The ClientID is provided to you by a CYREN representative along with the DNS server string and license key code.

Contacts

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

ctengine CYREN is a licensed SDK product featuring patented technology. CYREN's patented solution is protected by U.S. patent #6,330,590. RPD, Zero-Hour Protection, IPRep, ctipd, and ctwsd are CYREN trademarks of CYREN Inc. For more information, visit our website: www.cyren.com.