Inbound ctasd™ Implementation Guidelines

Checklist and Recommendations for the Integration Project Manager

CYREN Advanced Security Daemon (a.k.a. ctasd™) is a plug-n-play email-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. ctasd can be used to offer incoming email protection that enables CYREN OEM and ISP partners to prevent their customers or users from receiving spam. It can also be used to enable service providers the ability to detect and block outbound spam messages, thereby protecting their business reputation and avoid being blacklisted by other servers. ctasd can be integrated to deliver the following Inbound Mail Flow Services:

- Spam detection
- Virus outbreak detection
- Command Antivirus protection

Each service can be licensed and provisioned separately without affecting the other services. All the services, which share a single license key code, are provisioned on the CYREN Datacenter. Once provisioned, the partner may choose to disable one or more services locally for testing purposes.

The purpose of this document is to outline implementation guidelines and recommendations based on CYREN's experiences, for integrating ctasd with another messaging or security application.

Guidelines for All Services

License Key

The CYREN Datacenter is responsible for maintaining a vast repository of threat-related classifications and categorizations related to email and web security. ctasd communicates with the Datacenter to receive information such as spam and virus classifications. 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
- **OEM token:** A unique identifier (up to 35 alphanumeric characters) provided by the OEM partner

The OEM partner's identifier should distinguish between each user, device, or installation. A single ctasd daemon can provide single or multiple Inbound Mail Flow Services without affecting performance and accuracy. However, another ctasd daemon is required to provide single or multiple Outbound Mail Flow services (and vice versa). Once provisioned, the CYREN partner may choose to disable one or more services locally for testing purposes and then enable the service or services for actual production use. If using an OEM token, it should be unique for the lifetime of the host application and should not be changed so that the same OEM 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`

RefID

The RefID is a parameter that is returned by ctasd with every message classification. It contains a transaction tracing code that can help CYREN technical support track the reason for the classification. It is recommended that you create a mechanism to copy this value and add it to a special x-header of the message in order to provide better service to your customers, should they require CYREN to trace why a message was classified a certain way.

Note:	*Without this key, CYREN is unable to retroactively determine the reason why a message classification was returned and then reported as a detection mistake. Classifications are constantly updated to reflect the current status of an outbreak and only the most recent classification is retained in the Classification Warehouse.*

Site-Level Quarantine

In order to allow global management and diagnostics of blocked messages by system administrators, it is recommended that you develop site-level quarantine with the ability to release, delete, forward, and recycle messages that are not redirected to the recipients.

User-Level Quarantine

In order to allow user-level involvement, it is recommended that you create user-level quarantine. You can then create a method whereby users can access this quarantine to review and release non-threatening messages. You can also create a method for allowing users to create user-level policies for users to create policies for future handling of messages from the same source. Alternatively, you can create a mechanism to tag messages to users indicating the level of threat detection and forward these tagged messages to their Inbox folders to setup their own rules (such as via the Outlook rules wizard, etc.)

SNMP Counters

ctasd maintains many SNMP counters to monitor its performance and activities. In version 4.02, these counters have been updated and additional counters have been created. This functionality is not backwards compatible. This means, if you have previously created policies based on existing counters, it is possible that this policy must be updated to reflect the new counter name and/or functionality.

Guidelines for Spam Detection

Messages are divided into “good” and “bad,” as described in the table that appears below. “Bad” emails are spam messages that either come from known spammers, for example, zombies, or messages that contain spam patterns but are not from known spammers at the time the message is received. “Good” messages are those that are from trusted sources or those that contain no recognized spam patterns.

Note:	*The Service Provider/OEM partner is responsible for selecting and implementing external policy management for these or other options, as it chooses.*

Classification	Explanation	Optional Action(s)
Confirmed	Spam messages from known spam sources (e.g. zombies).	▪ Delete on arrival with or without generating a bounce-back message to the sender. ▪ Direct to site-level quarantine for the administrator to manage.
Bulk	Spam messages from sources that are not confirmed spammers.	▪ Direct to site-level quarantine for an administrator to manage. ▪ Direct to user-level quarantine for the end-user to manage. ▪ Tag with warning and forward to intended recipient.
Suspected	Messages that are sent to slightly larger than average distribution or are unidentified spam messages in the first few seconds of a massive spam outbreak.	▪ Forward to intended recipient.
Unknown	Messages for which ctengine does not have any incriminating information, and are therefore assumed to represent legitimate correspondence.	▪ Forward to intended recipient.
NonSpam	Messages that are confirmed, without doubt, as coming from a trusted source. This classification is very rarely used.	▪ Forward to intended recipient.
ValidBulk	Messages that are determined by the Datacenter to be valid bulk (e.g. solicited bulk messages such as newsletters.	▪ Forward to intended recipient

Note: *The Mail Sort feature enables better inbox management by distinguishing personal emails from valid, general mailings such as newsletters. When ctasd determines that an email contains solicited newsletters or similar bulk mailings, it returns with a classification of Valid Bulk.*

By default, the Valid Bulk classification is not enabled. In order to enable this classification, you must uncomment the ValidBulkEnabled parameter in the ctasd.conf and change the value to 1 (enabled). The default value is 0 (disabled).

LocalView Engine

For those customers who implement a dual-engine anti-spam strategy, CYREN's LocalView engine introduces a SpamAssassin-like scoring and threshold system that provides additional detection functionality. The LocalView combines each customer's Black and White lists and scoring preferences, CYREN-defined rules, and Custom Rules defined and managed by the CYREN customer, to provide maximum accuracy and detection. Information on managing these LocalView rules is detailed in the *LocalView Rules Management Guide.*

Spamd

In addition to its standard protocol, ctasd also supports a SpamAssassin-compatible protocol, referred to as Spamd. The Spamd protocol should be used when a Mail Server has built-in integration to SpamAssassin. In these cases, it may be easier to integrate with ctasd using the spamd protocol, which is compatible for use with the Exim Mail Server. Refer to the Inbound ctasd Integration Manual for details on the spamd protocol.

Guidelines for Virus Detection

Because virus outbreak detection services are designed to detect new virus outbreaks, it is highly recommended that you deploy ctasd after the message has already been scanned by your current anti-virus application.

When ctasd finds enough evidence to suggest the likelihood that a virus is present, it is often recommended that you hold the message until the next relevant anti-virus update instead of immediately deleting it (to avoid cases of false positives) or forwarding to the targeted recipients (to avoid cases of false negatives).

Holding the message until the next immediate anti-virus update might not always be the best tactic to use, if the anti-virus vendor has not had an opportunity to release the appropriate signature. Therefore, it is recommended that you determine the average response time for detecting new virus outbreaks for the particular anti-virus software in use. You can then calculate how long to hold the message before again passing it to the anti-virus software.

Note: *The Service Provider/OEM partner is responsible for selecting and implementing external policy management for these or other options, as it chooses.*

Virus Threat Level (VTL) Classification	Explanation	Optional Action(s)
Virus	The message contains characteristics of confirmed malware.	▪ Reject or delete the message. ▪ Peel off the malware from the message if you have the means to do this.
High	High likelihood of the message presenting a malware threat.	▪ Delete the message. ▪ Direct the message to your anti-virus quarantine (if applicable) for manual release by the administrator. ▪ Hold the message in a special queue for the next relevant anti-virus update.
Medium	Probable threat of virus in the message has been detected.	▪ Hold the message in a special queue for the next 2-3 relevant anti-virus updates. ▪ Forward to intended recipients.
▪ **Unknown**	▪ Threat for virus could not be determined at this time.	▪ Treat this as an email without a virus.
▪ **NonVirus**	▪ Confirmed that message does not contain a virus.	▪ Treat this as an email without a virus.

Reporting Classification Mistakes to CYREN

Although ctasd delivers a very high detection rate, users may occasionally feel that a message should have been classified differently. It is recommended that you implement a mechanism that enables your users to report these “misclassifications” back to the host application. By reporting any cases of false negatives and, more importantly, any cases of false positives to CYREN, you can improve the overall performance even further.

For more information about reporting classification mistakes review the *ctasd Integration Manual* and the *Reporting Classification Mistakes to CYREN* documents that are packaged with ctasd.

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

CTT01-500-911-078-R1

ctengine 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 trademarks of CYREN Software Ltd. For more information, visit our website: www.cyren.com.

Linux is a trademark of Linus Torvalds. FreeBSD is a registered trademark of Wind River Systems, Inc. COPYRIGHT AND PERMISSION NOTICE Copyright (c) 2014 , Daniel Stenberg, <daniel@haxx.se>. All rights reserved. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE

LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All other trademarks and registered trademarks are the property of their respective owners.