



**tiki**  
TECHNOLOGIES

Technology Brief 03/08 v.2.0

Solutions for a better Internet

## **Scora v.2.0: A Product Overview**

### **Contents:**

- ▶ **System Architecture and Overview**
- ▶ **The Scora Approach to Spam and Virus Filtering**
- ▶ **Administrative & User Features**

## Solutions for a better Internet

### Scora v.2.0

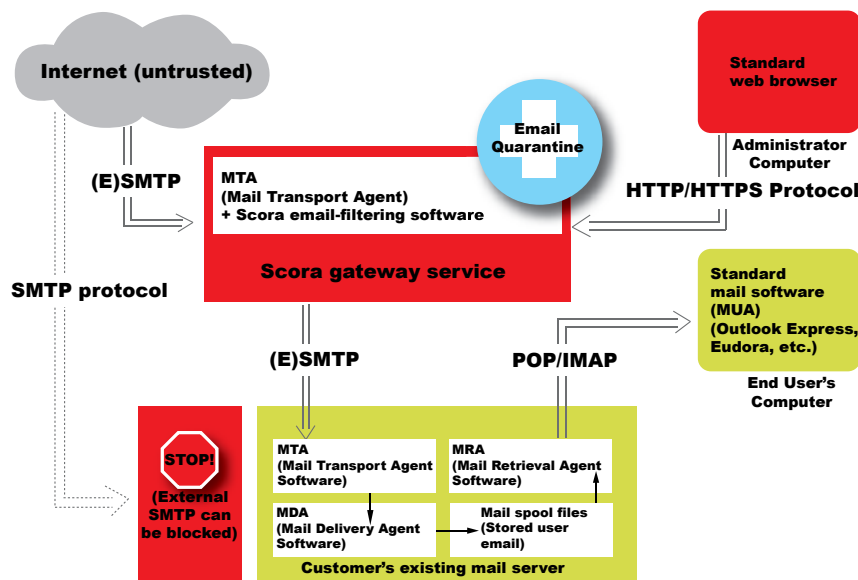
Powerful protection against email spam and viruses.

Scora is an email intrusion prevention service. Scora filters spam and viruses at an email gateway. It makes email more manageable, reducing costs and network risks for administrators and end users.

### System Architecture and Overview

Scora operates as a filtering gateway service that stands between your email server and the Internet. By configuring the MX (Mail Exchanger) records in your domain's DNS (Domain Name System), you direct all Internet mail servers and programs to route incoming mail for your domain via Scora. For further security you can configure your mailserver or firewall to reject all email connections except through Scora. The following diagram illustrates how Scora acts as an email firewall for your domain:

*Email data flow for Scora*



Scora distributes incoming mail simultaneously across multiple scanning servers for maximum performance, scalability, and fault-tolerance. Each incoming message is disassembled, checked against hundreds of rules and thousands of virus signatures, assigned a probability score of being spam, a virus, or unwanted explicit content, and finally assigned a disposition as determined by the administrator's and/or end user's preferences. It is then deleted or delivered to the desired mailserver or to a quarantine area.

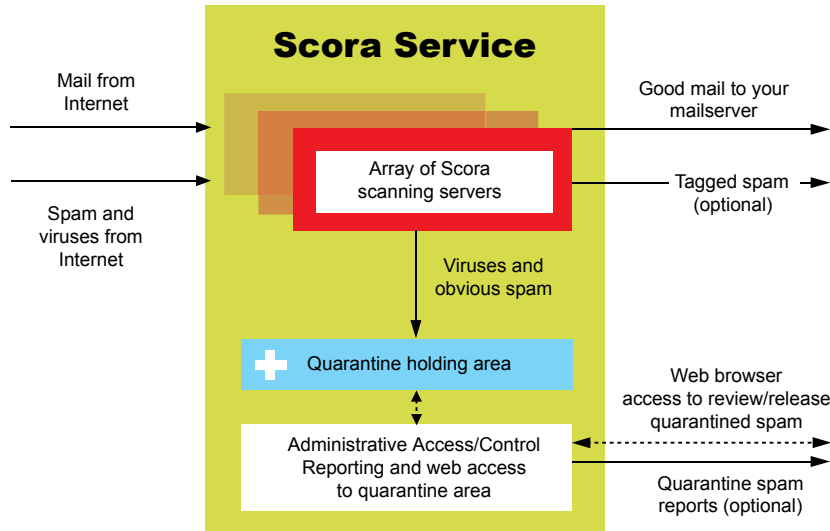
### KEY FACTS (Scora V.2.0)

- 98% accurate in identifying spam - more effective than Spam Assassin™\*
- Over 800 automatically optimized rules to identify spam
- Over 2600 rules to identify identity-theft 'phish' emails
- Over 156,000 signatures to identify viruses, updated every 2 hours
- <2 second pass through rate
- Supports individual message size of up to 50MB
- Identifies spam keywords delivered in email graphics
- 24X7 technical assistance

\* Scora 1.32 testing against SpamAssassin™ (v3.0.1), with SA's default settings for a binary determination of ham/spam (SA score > 5 = spam). SA: 96%.

## Solutions for a better Internet

(...System Architecture and Overview - cont'd)



### KEY FACTS

Scora takes over the “heavy lifting” for your email flow. The email-related bandwidth, storage and CPU demands on your network drop when Scora is used.

Scora runs on the Tiki Technologies server cluster. Incoming mail is load-balanced across a redundant array of high-performance servers which analyse the incoming messages and determine their handling. Message quarantine, report generation, web access, configuration and housekeeping tasks are all performed on a separate group of redundant servers to avoid bottlenecks in inbound mail processing. Internet connectivity is via 100Mb/s Ethernet connection to multi-homed T3 Internet backbone connections. Shared storage for quarantine access and configuration is provided by a Network Appliances Filer 740 with redundant power supplies. Power for the servers, storage, and switches is distributed across two different UPS sources, with generator backup.

(All technical details as of Spring 2008.)

### The Scora Approach to Spam and Virus Filtering:

Scora comes preconfigured for default filter settings that work exceptionally well as a starting point for all customers. Set them and forget them. Over time, some customers choose to increase or decrease the severity levels of the filters. Expert technical support is available for the administrator. Scora allows the administrator and/or the end user to easily develop and maintain a customized response to their email needs. Scora does not treat all spam equally. There are separate filters (which can be separately adjusted) for generic spam, viruses and spam with explicit content.

## Solutions for a better Internet

*(...Scora Approach to Spam and Virus Filtering - cont'd)*

### **The Scora Filtering Engine: Fast and Intelligent.**

Scora achieves superior anti-spam performance through a combination of filtering technologies.

As an email is assessed using these filtering technologies, a set of metrics is produced profiling the email's characteristics. Scora then applies a proprietary scoring system to this, weighing and combining scores according to administrator and/or end user preferences to arrive at a numerical score representing Scora's confidence level that the email is or is not likely to be spam. This numerical score (expressed on a scale of 0% to 100%, 100% being absolute certainty that an email is spam) is then compared to the thresholds and dispositions set by the administrator for the domain or by individual end users for their own email. The email is then handled in accordance with disposition preferences that correspond to that threshold level. Available dispositions include: normal delivery, subject flagged delivery, quarantine, and deletion. Subject flagged delivery also allows additional sorting options on the client side, as desired. All of this happens in the blink of an eye (less than 2 seconds on average from arrival to hand off to the customer's MTA. When used correctly, Scora relieves customer servers of most of the bandwidth and CPU usage caused by growing volumes of spam.

### **Key Filtering Technologies used in Scora v.2.0:**

Scora's capabilities are built up from a number of independent and cooperating modules or subsystems. This allows Scora to steadily advance over time as additional spam-recognition or processing modules or new subsystems are added.

Scora uses a combination of filtering technologies, enhanced by Scora's independent probability-driven scoring system. For instance, SpamAssassin™ is one of the components used by Scora. Since Scora is designed to allow individual tests (including SpamAssassin™ tests) to be recognized as indicators of more than one category of unwanted email, an email containing keywords that Spam Assassin would recognize only as generic spam can be further categorized by Scora as containing indicators of the Scora category of "explicit content". Scora will then route the email according to administrator and/or end user preferences for explicit content, which can be set independently from preferences for generic spam. In the same way, if an antivirus signature identifies an email as containing an identity theft "phish", Scora can classify and route it according to the administrator's preferences for "phish" content rather than mistakenly treating it as a virus.

This allows Scora to achieve synergistic increases in catch rate and effectiveness over the capabilities of any one technology.

#### **KEY FACT:**

Filter settings can be independently controlled for:

- Commercial Spam
- Explicit Content
- Viruses
- Phishes (Identity Theft)
- Domain-level filter settings, whitelists, and blacklists can be controlled by the domain's administrator; end users can also customize these for their own address.



## Solutions for a better Internet

*(Overview of Key Filtering technologies used in Scora v.2.0 cont'd)*

Scora uses the following anti-spam techniques:

- ▶ DNSBLs (DNS block lists), each independently scored
- ▶ Email header checks via pattern matching for known or probable indicators of spam or of desirable mail
- ▶ Email content checks for content/phrases that are probable indicators of spam or explicit content
- ▶ Email sender analysis against known spam-sending sources and known good sources of mail
- ▶ Email MIME format analysis for spam indicators and “signatures”
- ▶ Mailserver “hello” string format analysis against known spamware formats
- ▶ Shared complaint listing services including the Spamcop and Razor2 (Cloudmark) database
- ▶ Optional greylisting to delay mail from newly seen and untrusted sources
- ▶ Positive reputation services such as Habeas and IADB
- ▶ Open source antivirus software (Clam AV Scanning Engine)
- ▶ Antivirus style signatures for common phishes
- ▶ Optical Character Reader analysis of graphics in incoming mail
- ▶ Meta-analysis of content and domain together with IP and routing information to identify phishes

**KEY FACT:**

---

By using a combination of filtering technologies and techniques, Scora achieves a synergistic increase in effectiveness.

This entire suite of techniques can be applied:

<b>To identify spam</b>	<i>Via virtually all of the above techniques</i>
<b>To detect explicit content</b>	<i>Primarily via header and body content analysis</i>
<b>To identify “phishing” emails</b>	<i>Via sender analysis, header and body content analysis, and virus signature checks</i>
<b>To detect viruses and mass mailed worms</b>	<i>Primarily via virus signature checks, but also via email header and MIME structure analysis</i>



## Solutions for a better Internet

### Prefilter Blocking:

Scora offers built-in support for DNS block lists, which allows users to reject email from known spam sources immediately at the gateway. This is a powerful benefit for domains which already receive a high volume of spam, as you can avoid large volumes of obvious junk mail in your users' quarantine.

This feature can also be turned off completely at the client's discretion. There are four severity levels of prefilter blocking available, corresponding to different subsets of the master list available through Scora:

### KEY FACT:

By allowing users to choose the degree of blocking, or turn it off completely, Scora offers a level of disclosure and control that is very customer friendly.

#### None

- Prefilters disabled

#### Minimal

- Sender address domain must be valid and exist
- Mailserver 'hello' checked against known bad domains
- IP checked vs CBL composite bot-net blocklist (cbl.abuseat.org)
- IP checked vs DSBL proxy list (list.dsbl.org)

#### Usual (default setting)

- All Minimal Prefilter checks are run plus:
- Mailserver "hello" format checked for known spamware formats
- IP checked vs XBL composite open relay/proxy/boy-net blocklist (incorporating CBL and NJABL blocklists)
- IP checked vs Spamhaus list (sbl.spamhaus.org)
- IP checked vs PBL policy blocklist (en-user IP addresses not authorized to send email directly)
- IP checked vs bhnc.njabl.org (suspected spam proxies)
- Greylisting - requires temporary delay of mail coming to a given user from a previously unknown source

#### Maximum

- All Minimal and Usual Prefilter checks are run plus:
- Sender address domain checked against list of known pure spam-source domains
- Sending server hostname checked against list of known pure spam-source domains
- IP checked vs Spamcop blocklist (major source of current reported spam)



## Solutions for a better Internet

### Administrative & User Features:

Scora is configured and maintained using a web-based administration system. The user interface is designed to give the email administrator and/or the end user quick and informed access to current settings, and the ability to fine tune them as needed. Key aspects to the administrator features include:

**System Default Settings.** The system default settings are preset for new customers. These represent a cautious but effective severity level for spam identification. For reference, a score of 100% would indicate absolute certainty that an email is spam. An administrator can easily change a domain's spam or explicit content filter to a more aggressive setting, simply by clicking the "aggressive" or "very aggressive" button on the filtering options page. Even with the "very aggressive" option, it is rare for mail to be misclassified.

	Generic Spam	Explicit Content	Viruses	Phish
▶ Deliver Normally:	< 99.5%	< 99.5%	< 99.5%	< 99.5%
▶ Subject Flag/Deliver:	99.5%	99.5%	99.5%	99.5%
▶ Quarantine:	99.999%	99.999%	99.99%	99.99%
▶ Delete:	NEVER	NEVER	NEVER	NEVER
▶ Reject at gateway:	"Usual" setting for Prefilter Blocking enabled for default settings.			

**Filter Updates and Network Monitoring.** Scora antispam rule sets are updated on an ongoing basis. Generally there are 1-2 rule updates or minor updates per month, and 3 to 5 major updates a year. Antivirus rulesets are updated every 2 hours. Updates are included with the service. The Scora network operations center is electronically monitored 24 hours a day.

**Quarantine.** The system default settings (preset for new customers) can be adjusted to quarantine at a lower threshold, or a higher one. The quarantine is optional; suspect email flagged as probable spam can simply be tagged and delivered, which would mean a 0% chance of false positives but a high tradeoff in the volume of unwanted email.

**Supports exempt users.** There are business scenarios in which a few addresses should not be filtered in any way. Scora supports a mix of filtered and exempt email users at your domain.

### KEY FACT:

Scora can act as a "set and forget" system or be as highly customized as the customer wants it to be.

### KEY FACT:

- Scora quarantine features:
- Off-site storage of quarantined messages
  - Detailed reports
  - 1- click release
  - Up to 30 day off site storage



## Solutions for a better Internet

**Reports.** Generate reports for administrators and/or end users to review the quarantine for false positives. Reports include the date, sender's email address and title of quarantined email. They are a quick way for end users to make sure that a valid email was not misclassified as spam. Reports include an embedded link that allows the person reviewing the report to release an individual email from quarantine for delivery to the original recipient with just one click. Reports also include a full count of all email-handled for that address and how it was handled by Scora.

**Offsite storage of quarantine.** Quarantined email is stored on Scora's network-attached storage system, not on customer's network. This significantly reduces the storage demands on the client's mail server and also provides a safe place for the storage of dangerous computer viruses and worms, far from the customer computers. Quarantine storage limits may be set for up to 30 days or as little as one day. The default is 20 days.

**Broad range of whitelisting options.** The headers for each email examined by Scora retain a record of the rules "tripped" by the email. Should a valid email be misclassified as spam, a whitelist entry (sometimes in conjunction with adjustments to the prefilter blocking settings) will make sure this does not recur. Tiki Technologies technical support can assist customers to interpret these and to base whitelisting entries on the right parameters to ensure the best possible outcome. Scora allows whitelisting by email address, domain, IP, hostname, mail server domain, mail server hostname, mail server "hello" ID, and mail server "hello" domain. The whitelist can be set at the domain level, for a number of an administrator's domains, or for an individual address by an end-user.

**Broad range of blacklist options.** Scora uses its many data sources to dynamically adapt to catch and block new sources of spam. However, if spam from some source continues to get past Scora to one of your email addresses, you have options to block it with your own blacklist. You can configure Scora to blacklist email by sender address or domain, by mail server IP address, hostname, or domain, or by mail server "hello" ID or domain. Blacklisted mail goes directly to the quarantine where it can be retrieved in the event of an error. The blacklist can be set at the domain level, for a number of an administrator's domains, or for an individual address by an end-user.



## Solutions for a better Internet

**Keyword blacklisting.** Not all domains and users get the same level or varieties of spam - some domains end up targeted for particular kinds of spam on certain topics. If a particular domain is getting a specific variety of spam consistently sharing certain keywords, and Scora does not consistently detect and block all of it, the domain administrator can block it by specifying those keywords. All email to that domain containing the specified keywords will be sent directly to the quarantine; it will still show up in the periodic report and be available for review and release if necessary. (Note: Scora recommends very cautious use of this feature, to avoid mistakenly categorizing valid mail as spam.)

**Greylisting.** Scora allows a domain administrator to enable greylisting on their domain by selecting the “usual” or “aggressive” level of pre-filter blocking. Greylisting is a powerful defense against spam sent by specialized spam software, especially the spam coming from the millions of virus-infected PCs around the world. When greylisting is enabled, on the first attempt to deliver a certain email from a given IP address to a given user, Scora will respond to the sending mailserver requesting a 5 minute delay. On the next attempt to deliver it, Scora will accept the email. The software used for sending spam is usually unable to retry and so the spam never gets through while mail from real senders does. Once a server has delivered email to Scora a few times, Scora automatically whitelists the IP address so mail from that mailserver is never delayed again. (Note: greylisting does delay incoming mail from new sources, and is not an appropriate technique for domains which want only light filtering; Scora does not allow greylisting to be enabled with the “minimal” or “none” prefilter settings.)

**5 day emergency queue service.** Should the destination email server for a domain served by Scora fail to accept email, all mail for the domain name will continue to be filtered and be queued by Scora for up to 5 days. The 5 day interval was chosen for maximum protection of customer business continuity.

**Repels “dictionary attacks”.** Scora refuses email sent to non-existent addresses at your domain, foiling a frequently used spammer tactic of making up names and hammering your mail server.

**Reporting support for email aliases.** One email address may act as the receiving mailbox for many aliases or mailing groups. Rather than have to go through a separate Scora report for every address your mailbox receives email for, the userlist interface allows the administrator to group these together, sending one report for the entire group of email addresses.



**tiki**  
TECHNOLOGIES

Technology Brief 03/08 v.2.0

## Solutions for a better Internet

### Conclusion

Scora is an effective guardian against the negative business effects of email spam and viruses. Scora combines ease of use with advanced features to serve a wide range of customers and is highly customizable by the administrator and/or the end user. Scora works for any domain name, whether it points to a customer mail server or to any ISP. By acting as the Internet-facing gateway for email, Scora takes over the CPU, bandwidth and storage-intensive aspects of spam and virus filtering, delivering a clean, efficient email feed. This reduces end user effort and hassle, restoring productivity to email and reclaiming it as the powerful business tool it has the potential to be. Scora is available for domain serving as few as five addresses, or tens of thousands of addresses. With Scora, customers in Hawaii get the ability to reach support staff right here on the island, not in an outsourced call center somewhere else in the US or in the world. Your Scora mailservers are hosted here in Honolulu, not in a remote mainland data center

Potential clients may sign up for a free, one month trial of Scora online:  
<http://www.tikitechnologies.com>

Scora is made by PDC Systems  
629a Pohukaina Street  
Honolulu, Hawaii 96813

Website: <http://www.tikitechnologies.com>  
Email: [scora@pdcsystems.com](mailto:scora@pdcsystems.com)

Phone: 808.537.1234  
Facsimile: 808.537.6644