# TUNING SYMANTEC BRIGHTMAIL ANTISPAM ON THE SUN FIRE™ T2000 SERVER

Alan Yoshida, Sun Market Development Engineering
Ramin Moazeni, Sun Market Development Engineering
Steve Gaede, PointSource Communications

Sun BluePrints™ OnLine —
October 2006


Part No 820-0132-10
Revision 1.0 10/24/06
Edition: October 2006

# Table of Contents

# Tuning Symantec Brightmail AntiSpam on the Sun Fire™ T2000 Server

Electronic mail is a business-critical function in virtually every enterprise, and it is also one that is under constant attack. Well-known viruses such as Melissa, and worms like SoBig have propagated through e-mail and have disrupted user PCs and corporate networks worldwide. Fraudulent e-mail messages find their ways into inboxes and tempt unsuspecting users into divulging personal information at phishing sites. As companies recognize that their intellectual property can easily leave their premises through e-mail messages, filtering outbound and internal messages is becoming as important as protecting an organization from incoming traffic.

No e-mail problem is more troublesome or visible, however, than unsolicited bulk e-mail, commonly known as *spam*. Spam can have a huge impact on employee productivity, and because it also can serve as a vehicle to deliver malicious content including viruses, worms, and phishing attacks, many organizations tackle the spam problem as a first step in implementing a comprehensive e-mail security strategy.

In recent years, the volume of spam has risen to epidemic proportions. Although estimates of the ratio of spam to legitimate e-mail vary, it is widely agreed that it makes up at least 50 percent of e-mail traffic today. This presents a particular challenge to anti-spam software. It must be intelligent enough to filter out a very high percentage of spam, while leaving virtually all legitimate e-mail messages intact. As spammers continue to invent techniques in hopes of circumventing anti-spam software, the intelligence of anti-spam technology — and the processing power needed to detect and eliminate it — must stay ahead.

The combination of Symantec Brightmail AntiSpam (SBAS) software and the Sun Fire™ T2000 server is particularly well suited to the demanding task of spam filtering. SBAS works in conjunction with an enterprise Message Transfer Agent (MTA) such as the Sun Java™ System Messaging Server to analyze each incoming message and determine whether it should be classified as spam. SBAS uses standard methods such as heuristics and pattern matching, augmented with proprietary filtering methods including advanced signature technologies and reputation-based source filters updated in real-time as Symantec analyzes and prepares countermeasures based on observations of current spam traffic. In order to process large volumes of spam without impacting the throughput of an enterprise MTA, multiple messages must be processed concurrently — and concurrent processing of multiple threads is where the Sun Fire T2000 server excels. Based on the UltraSPARC® T1 processor with CoolThreads™ technology, a single eight-core processor can handle up to 32 threads concurrently, giving a significant performance advantage over typical single-threaded processors. Indeed, out-of-the-box, with no tuning, Brightmail on a Sun Fire T2000 server with a single eight-core UltraSPARC T1 processor outperforms a Sun Fire V240 with two single-threaded UltraSPARC processors by more than 50 percent.

In order to best take advantage of the advantages of Chip Multi-Threading (CMT) in the UltraSPARC T1 processor, administrators should make some relatively simple tuning adjustments to SBAS software. The result of taking the simple steps described in this Sun BluePrints™ article yielded a 5.2x improvement over the same installation with no tuning.

This Sun BluePrints article provides background information on SBAS software and the Sun Fire T2000 server, the configuration used for performance measurements, the challenges presented by benchmarking anti-spam software, and the actual steps used to tune the hardware/software combination to achieve the reported performance levels.

## How this Article is Organized

This Sun BluePrints article is organized into the following sections:

- “A Unique Match of Technologies” on page 2 briefly describes SBAS and the Sun Fire T2000 server.
- “Test Configuration” on page 4 describes the software and hardware configuration used to measure SBAS performance during the tuning effort.
- “Your Mileage May Vary” on page 5 discusses the differences between the test configuration and the real-world situations in which SBAS will be installed, and why different customers may observe different performance.
- “Tuning SBAS on the Sun Fire T2000 Server” on page 6 details the steps that were taken in order to achieve the 5.2x speedup over the server’s out-of-the-box configuration.
- “Summary” on page 7 provides a recap of the results and how the Sun Fire T2000 server is able to deliver outstanding performance.

## A Unique Match of Technologies

The Sun Fire T2000 server and SBAS software is a unique match of technologies. SBAS owes its accuracy to the sophisticated rules and heuristics used to detect and eliminate spam. In order to achieve this level of accuracy, the software requires significant CPU time to evaluate each incoming e-mail. At a time when most Information Technology (IT) organizations are striving to deploy ever more applications in data centers that are often at the limit in terms of space, power, and cooling capacity, the Sun Fire T2000 server offers a refreshing new option. Designed for highly multithreaded, network throughput-intensive applications, the Sun Fire T2000 combines high performance and low power consumption in the same space-efficient and cost-effective package.

### Sun Fire T2000 Server

The Sun Fire T2000 server is powered by the UltraSPARC T1 processor with CoolThreads technology. Unlike traditional single-threaded processors, the UltraSPARC T1 processor is designed to support multiple threads per processor core, with the ability to rapidly switch between active threads as other threads stall waiting for memory requests to be fulfilled. Sun’s CMT approach enables each processor core to switch among four active threads on each clock cycle. The result is a processor pipeline that is active doing useful work a higher percentage of the time, resulting in both excellent performance and lower power consumption for the amount of work done. The Sun Fire T2000 server can be configured with a single processor having four, six, or eight processor cores. Equipped with eight cores, the result is 32 logical processors per server. In addition to the performance benefits described in this article, IT organizations can also enjoy the power savings that result from the UltraSPARC T1 processor’s design. While an Intel Itanium processor running at 1.9 GHz consumes 180 watts of power, an UltraSPARC T1 processor running at 1.2 GHz consumes only 79 watts, less than half the power.

The Sun Fire T2000 server is capable of supporting up to 32 GB of main memory and up to four hot-pluggable 2.5” SAS disk drives. The server includes three PCI-Express expansion slots, and two PCI-X slots. Reliability, availability, and serviceability are further increased through the use of redundant hot-swappable power supplies.

**Symantec Brightmail AntiSpam**

Symantec Brightmail AntiSpam provides complete server-side anti-spam and anti-virus protection. It processes incoming e-mail traffic, identifying, analyzing, and discarding spam and virus attacks before they inconvenience users and overwhelm internal networks and e-mail clients. SBAS runs each incoming e-mail message through a gauntlet of filters designed to eliminate more than 95 percent of spam with an accuracy of 99.9999 percent — meaning that fewer than one false positive will occur in 1 million e-mail messages. This high level of effectiveness along with pinpoint accuracy helps ensure that users continue to receive the legitimate e-mail messages they need, while keeping the vast majority of spam and virus-laden e-mails from ever reaching their inboxes.

SBAS uses a combination of filtering technologies, some of which are optional and can be configured by on-site administrators, and the majority of which are created by Symantec and updated on a minute-by-minute basis through a secure connection to one of Symantec’s worldwide global operations centers. The types of filters are illustrated in Figure 1, with optional, locally-defined filters in orange. The remaining filters are managed and maintained by Symantec, and updated based on constant monitoring of special trap accounts strategically located on the Internet. Once an e-mail has been reviewed and assigned a spam classification, it can be delivered normally, delivered with modified headers, deleted, delivered to the recipient’s spam folder, saved or forwarded for administrator review, or quarantined to a Web-based interface where users can view caught spam.

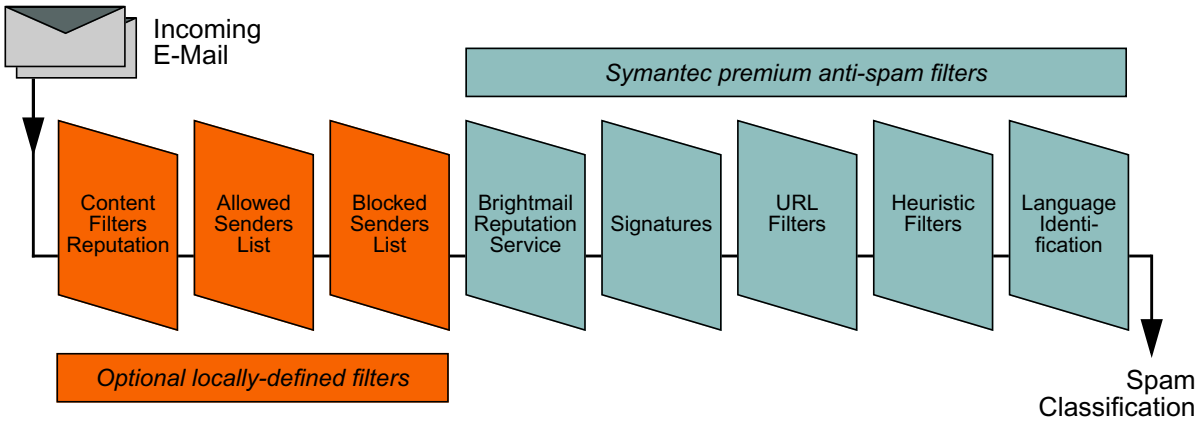



*Figure 1. SBAS runs each e-mail message through a gauntlet of filters, resulting in a spam classification that determines the disposition of each message.*

## Test Configuration

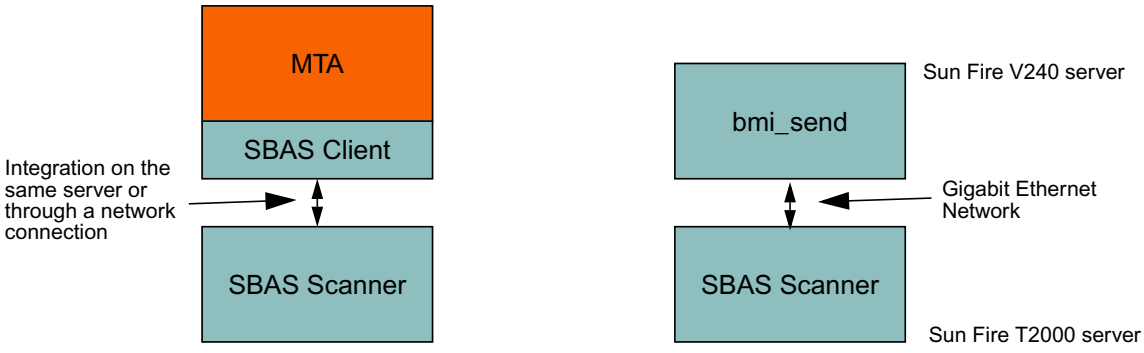
SBAS integrates with MTAs including the Java System Messaging Server, Sendmail, Microsoft Exchange, and Lotus Notes. A typical deployment scenario places SBAS on a gateway system, filtering all incoming e-mail and transferring the filtered e-mail to a layer of MTAs for local mail delivery. The software is flexible and scalable enough that it can be deployed in scenarios ranging from integrating with a single, central MTA, to one in which a high-availability, load-balanced group of MTAs process messages in parallel.

SBAS integrates with MTAs through an MTA-specific client that uses the Brightmail Engine Application Programming Interface (API) to transfer messages to the SBAS Scanner for analysis (Figure 2a). For the purpose of evaluating SBAS performance and its response to different tuning parameters, we used a simplified configuration where Symantec's `bmi_send` load-generation tool is used drive a synthetic e-mail workload through the SBAS Scanner using the same interfaces that an MTA would use (Figure 2b).

### Load Generator Configuration

We used a Sun Fire V240 server with two 1 GHz processors and 4 GB of main memory to generate the synthetic e-mail workload. The load generator, `bmi_send`, can be tuned to apply an e-mail workload using a specified number of threads. Varying the number of threads simulates a higher or lower message throughput from an MTA. The load generator was connected to the SBAS Scanner using a dedicated Gigabit Ethernet link.

The synthetic workload was created by Symantec by mixing a combination of valid e-mail messages with actual spam captured by e-mail trap accounts that Symantec maintains for the purpose of gathering and analyzing spam. The workload contains 4800 messages, with an average message size of 30 KB.




*a) Typical deployment with MTA integration.* *b) Test configuration using bmi_send*

*Figure 2. Under normal circumstances, SBAS integrates with an MTA; for test purposes, Symantec's bmi_send load-generation tool replaces the MTA and SBAS client.*

### System Under Test

The server used to host the SBAS Scanner was a Sun Fire T2000 server with a single 8-core, 1.2 GHz processor, 16 GB of main memory, and two 73 GB internal SAS disk drives. The server was configured with the Solaris 10 6/06 Operating System and SBAS 6.0.4.

For the purpose of comparison, a Sun Fire V240 with two 1 GHz processors and 4 GB of memory was used with the Solaris 10 1/06 Operating System and SBAS 6.0.4.

## Your Mileage May Vary

Computer system performance measurements are typically performed in laboratory situations using workloads that are representative of actual customer workloads. They give a good sense of relative performance between systems and the impact of changes such as the tuning steps described in this Sun BluePrints article. They do not, however, exactly predict the performance that customers will see in real-world deployments. In the case of benchmarking and tuning SBAS, customers are likely to see their own performance vary up or down from the measurements presented in this article for a number of reasons:

- *Every workload is different.*

  The e-mail workload driven by `bmi_send` was derived from actual spam captured by Symantec's e-mail trap accounts, and from actual e-mail sent to Symantec's corporate headquarters. The nature of spam is constantly changing, as is the amount of processing time needed to determine whether an e-mail message is spam. Likewise, average e-mail message sizes vary over time, and from company to company. Although every effort was made to make the body of e-mail used by bmi_send representative of actual current e-mail, larger or smaller average message sizes will have an impact on SBAS performance.

- *Real-world configurations are different.*

  The system configuration used to measure and tune SBAS performance did not include an MTA. The same API was used to drive the synthetic workload as is used in real-world configurations, but the complexities of real MTAs could cause overall e-mail handling performance to vary from the values reported in this article. For example, MTAs increase the overall CPU time and latency for processing each e-mail message, and any delay transmitting messages to or from the SBAS Scanner could cause overall performance to fall below the measurement for the Scanner alone. The best way to evaluate this variable is to consider the performance numbers reported in this article as representative of SBAS performance when coupled with a well-tuned MTA.

- *Anti-spam rules are constantly changing.*

  One of the key benefits of SBAS is that the rules and heuristics used to process e-mail are updated as often as every 5-10 minutes. As Symantec observes new types of spam arriving in e-mail trap accounts, it uses both automated and manual procedures to update rule sets and effectively eliminate the new type of spam. These rule set updates may change the order in which rules are applied, increasing efficiency for today's most commonly-used techniques, and they may include specific new rules or heuristics for detecting some of the more sophisticated spam.

  Customer SBAS implementations access these rule-set changes by periodically contacting Symantec logistics servers over an SSL connection. Although the benchmark used in this tuning exercise kept the body of e-mail constant, the SBAS rule set was not held constant, so there could be variations even between sets of measurements due to automated changes in the rule sets. As a result, the performance measurements reported in this article should be considered as guidance, and not as an absolute value

that any specific customer site should see. Your mileage may vary, and it may vary higher or lower than the numbers reported here.

## Tuning SBAS on the Sun Fire T2000 Server

Sun installed SBAS onto the Sun Fire T2000 server running the Solaris 10 6/06 Operating System, and also onto a dual-processor Sun Fire V240 running Solaris 10 1/06 (see “Test Configuration” on page 4). The tuning steps were developed by testing and experimenting with a wide range of parameters and values, and the results of that experimentation is presented here.

### Initial Installation Performance

With an ‘out-of-the-box’ installation, `bmi_send` was configured to maintain 210 concurrent connections when driving the SBAS implementation on the Sun Fire T2000 server. The base throughput was 18 messages/sec. For comparison, the same body of e-mail was used to drive the Sun Fire V240 server, achieving a base performance of 11.4 messages/sec. Out of the box, the Sun Fire T2000 server outperformed the Sun Fire V240 server by 58 percent.

### Increasing Service Threads

SBAS creates a separate thread to process each incoming e-mail message up to a limit specified by the parameter `maxServiceThreads`. The higher the `maxServiceThreads` parameter, the more messages that SBAS can process in parallel. The default maximum value is 5. With the ability of the UltraSPARC T1 processor to handle up to 32 threads concurrently in the processor itself, the default thread limit is obviously low. Experimentation showed the best results with 150-200 threads. With the value set to 180 threads, SBAS handled 57 messages/sec. This more than tripled the software’s spam-processing capability with a factor of 3.17x the base performance.

The `maxServiceThreads` parameter value is stored in the file `/opt/symantec/sbas/Scanner/etc/bmiconfig.xml`. Use a text editor and locate the following line:

```
<program xsi:type='bmserverType' name='bmserver'>
```

After the line above, and before the end of the section noted by the next `</program>` line, add a line:

```
<maxServiceThreads>180</maxServiceThreads>
```

### Deterministic Finite Automata (DFA)

The `DFA` parameter dictates whether some heuristics are pre-compiled in order to speed performance at the expense of using more memory. The default value conserves memory by not pre-compiling heuristics. After changing the `DFA` parameter to pre-compile heuristics, performance increased from 57 messages/sec. to 84 messages/sec., an improvement of an additional 47 percent.

The DFA parameter value is stored in the file /opt/symantec/sbas/Scanner/etc/bmiconfig.xml. Locate the line:

```
<DFA enabled='false'/>
```

and modify it to:

```
<DFA enabled='true'/>
```

**Integrating Multi-Threaded Malloc**

Mtmalloc is a version of the standard UNIX® malloc memory allocation library that is especially tuned for multithreaded programs. The Solaris OS mtmalloc library is tuned to minimize lock contention resulting in a lower probability that a thread will be suspended while waiting to obtain a lock within the memory allocation library. Changing the malloc library used by SBAS resulted in an increase from 84 messages/sec. to 94 messages/sec., an improvement of an additional 12 percent.

To change the malloc library used, change the LD_PRELOAD environment variable to point to the mtmalloc shared library. This can be done by modifying a set of shell commands that set environment variables for SBAS located in: /opt/symantec/sbas/Scanner/etc/brightmail-env. Add the following lines to the file:

```
LD_PRELOAD=libmtmalloc.so
export LD_PRELOAD
```

## Summary

Eliminating spam is one of the top priorities for IT organizations implementing a comprehensive e-mail security policy. Spam not only saps employee productivity, it can put user workstations, user personal information, and enterprise networks at risk. As the volume of spam and the sophistication of spammers increases, so does the processing power required to filter out virtually all unsolicited bulk e-mail messages while minimizing the risk of false positives.

One potent combination of technologies for fighting spam is SBAS and the Sun Fire T2000 server. SBAS integrates with the leading mail transfer agents, examines every incoming e-mail, and provides a spam classification that can be used to direct the disposition of each message. SBAS gains much of its power from the near real-time filtering rule updates based on the latest spam techniques for which Symantec is continuously developing countermeasures. Software such as SBAS must be highly multithreaded in order to process large volumes of spam concurrently, and no commercially-available microprocessor has the ability to process more concurrent threads at a hardware level than the UltraSPARC T1 processor with CoolThreads technology.

Most commercial, multithreaded software strikes a balance between increasing throughput by using a large number of threads, weighted against the increase in costly context switch overhead that is a hallmark

of typical single-threaded, highly pipelined processors. In contrast, the UltraSPARC T1 processor thrives on multiple threads, with a single 8-core processor able to handle 32 threads concurrently. Most commercial software needs some tuning to best utilize a processor with zero internal thread-switching overhead, and SBAS is no exception. After tuning both the SBAS operating parameters and the Solaris OS shared library environment, Sun was able to increase performance from an out-of-the-box 18 messages per second to 94 messages per second, a 5.2x improvement (Figure 3). Comparing the tuned Sun Fire T2000 performance to out-of-the-box Sun Fire V240 (dual processor) performance, an 8.2x increase was achieved. Most of the performance improvement is directly related to increasing the thread count in SBAS and reducing the contention for locks that arises from having a large number of active threads.

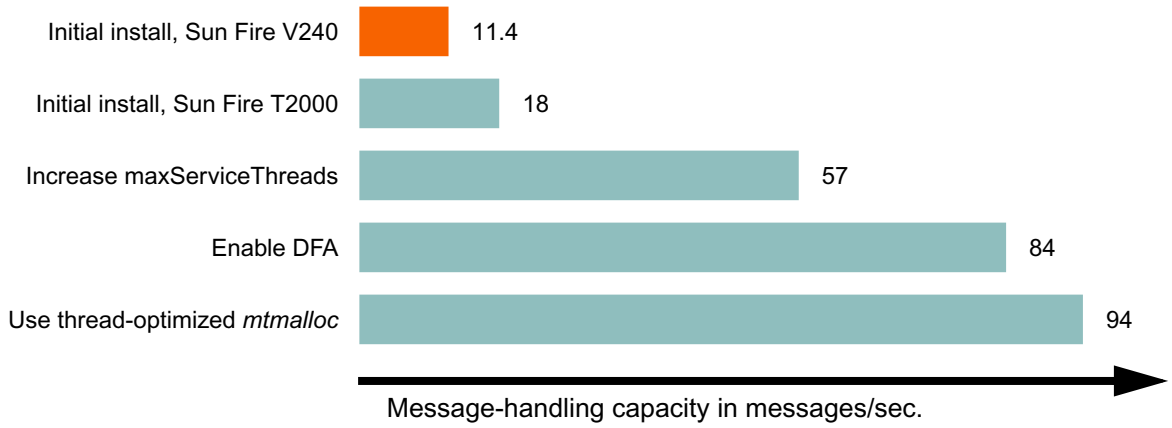



*Figure 3. The bottom line: tuning the SBAS Scanner yielded a 5.2x improvement over the initial installation on a Sun Fire T2000 server, and an 8.2x improvement over the initial install on a Sun Fire V240 server.*

As with any performance measurements made with synthetic workloads, customers need to remember that their mileage may vary. Every e-mail workload is different, spam techniques and countermeasures change in real time, and real-world configurations vary from the test configuration used in Sun's laboratories. Nevertheless, the series of tuning steps and their results give an indication of the kind of performance improvement that the Sun Fire T2000 server can deliver in comparison to traditional, highly pipelined microprocessor-based servers.

## About the Authors

Alan Yoshida is a Staff Engineer in the Market Development Engineering group at Sun Microsystems. As the lead engineer for the Symantec relationship within MDE, Alan's primary responsibility is helping to make sure that Symantec products run well on Sun platforms.

Ramin Moazeni is a Member of Technical Staff in the Market Development Engineering group at Sun Microsystems. He has been working with independent software vendors on performance engineering and in porting of their applications onto Sun platforms.

Steve Gaede is a technology consultant and writer who has lent his engineering and technical marketing expertise to various projects at Sun Microsystems since 1994. He works through PointSource Communications and his technically-focused company, Lone Eagle Systems, Inc.

## Acknowledgments

The authors would like to thank Symantec its support from configuration and tuning suggestions to the body of e-mail used in the tuning process. In particular, thanks to Tom Anderson, Jason Grauel, Matt Hartwell-Herrero, and Matt Steele.

## References

Information on the Sun Fire T2000 server is available at:

- `http://www.sun.com/products-n-solutions/hardware/docs/Servers/coolthreads/t2000/index.html`

A power calculator for the Sun Fire T2000 server is available at:

- `http://www.sun.com/servers/coolthreads/t2000/calc.`

Information on Symantec Brightmail AntiSpam is located on Symantec's Web site at:

- `http://www.symantec.com/enterprise/products/overview.jsp?pcid=1008&pvid=835_1`

## Ordering Sun Documents

The SunDocs℠ program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals through this program.

## Accessing Sun Documentation Online

The `docs.sun.com` web site enables you to access Sun technical documentation online. You can browse the `docs.sun.com` archive or search for a specific book title or subject. The URL is `http://docs.sun.com/`

To reference Sun BluePrints OnLine articles, visit the Sun BluePrints OnLine Web site at: `http://www.sun.com/blueprints/online.html`