

Accelerated Anti-Spam Symantec Brightmail AntiSpam on the Sun Fire™ T2000 Server



Highlights

- The combination of Symantec Brightmail AntiSpam and the Sun Fire™ T2000 server is a potent tool for enterprise-grade spam, virus, and content filtering.
- Symantec Brightmail AntiSpam is server-side anti-spam technology that stops spam before it can clog networks, servers, and inboxes.
- Constantly updated with current filtering rules from the Brightmail Logistics and Operation Center, Symantec Brightmail AntiSpam stays ahead of spammer tactics.
- Filtering every incoming e-mail is an inherently multithreaded operation. The combination of the Sun Fire T2000 server, the UltraSPARC® T1 processor, and the Solaris™ Operating System is the perfect match for high anti-spam throughput.
- Tuning this solution to best utilize the UltraSPARC T1 processor's ability to concurrently execute up to 32 threads yields a 5.2x improvement over an out-of-the-box configuration.



Unsolicited bulk e-mail, or spam. The trash strewn across the Internet by increasingly cunning spammers that can clog networks, servers, and inboxes. Even worse, it can deliver viruses, worms, Trojan horses, and subject users to phishing attacks. Fighting spammers means keeping your technology ahead of theirs — which means using highly-intelligent, self-updating anti-spam technology. Software smart enough to eliminate virtually all of your spam, yet leave legitimate e-mail untouched requires a lot of CPU horsepower — especially when, as experts agree, at least 50 percent of your incoming e-mail is unsolicited bulk e-mail.

Fortunately, between Symantec Brightmail AntiSpam software and the Sun Fire™ T2000 server powered by the UltraSPARC® T1 processor with CoolThreads™ technology, Sun has a high-performance solution that doesn't break your space, power, or cooling budget.

Sun and Symantec have worked together to make this combination of technologies work even better together. Symantec Brightmail AntiSpam is highly threaded, network throughput-oriented software that presents just the kind of problem that the UltraSPARC T1 processor loves to solve. With the capability to support up to 32 concurrent execution threads in a single eight-core processor, a properly tuned deployment can process more than 90 messages per second.

Introducing Symantec Brightmail AntiSpam

Symantec Brightmail AntiSpam (SBAS) provides complete server-side anti-spam and virus protection. It processes incoming e-mail traffic, identifying, analyzing, and defusing spam and virus attacks before they inconvenience users and potentially overwhelm internal networks, servers, and e-mail clients. SBAS protects 9 of the top 12 ISPs and over 100 billion e-mail messages per month.

Because it is a server-side solution, SBAS can stop spam and other malicious attachments before they can compromise security, putting the responsibility for enterprise security back into the data center rather than on individual users and their desktop systems.

A gauntlet of filters

SBAS runs each incoming e-mail through a gauntlet of filters designed to eliminate 95 percent of spam with an accuracy of 99.9999 percent — meaning that fewer than one false positive should occur in one million messages. This high level of effectiveness, along with pinpoint accuracy, helps users get the legitimate e-mail messages they need, while keeping the vast majority of spam and virus-laden messages from their inboxes.

SBAS implements four types of filters: anti-spam filters, content filters, allowed and blocked sender lists, and anti-virus filters. Some of the filters are optional and can be defined on a per-site basis, with the majority created by Symantec and updated every 5-10 minutes through a secure connection to one of four worldwide Brightmail Logistics and Operation Centers (Figure 1). Symantec captures spam in real time using spam-trap accounts and analyzes them using both automated and manual techniques, developing countermeasures that are then provided to customers through automated updates.

Filtering technologies

Filtering technologies used by SBAS include:

- *Content filters* that are written to meet the needs of individual organizations
- *Allowed and blocked sender lists* that can be locally defined
- *Blocked senders* defined by the Brightmail Reputation Service, including trusted and blocked IP addresses and domains
- *Signatures*, an accurate approach that identifies the underlying ‘DNA’ of spam, helping to defeat HTML-based and other evasion tactics used by spammers
- *URL filters* that match embedded URLs with a database of known spam and phishing URLs
- *Heuristics* that target patterns commonly found in spam

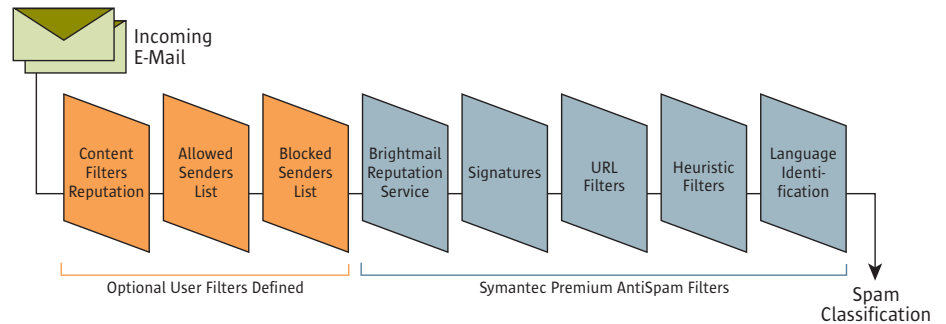


Figure 1. Symantec Brightmail AntiSpam runs each e-mail through a gauntlet of filters, some of which are locally defined, and some of which are updated from the Brightmail Logistics Center.

- *Language identification* that allows messages to be filtered on the basis of the language used

Spam classification

Once an incoming e-mail has passed through the filters defined by Symantec and those defined on site, it exits with a spam classification that can be used to dictate the final disposition of the message. Options include:

- Deliver the message normally
- Deliver with modified headers that can be used by e-mail clients in classifying messages
- Delete the message
- Deliver to the recipient’s spam folder
- Save or forward for administrator review
- Send to the Brightmail Quarantine, an optional Web-based interface where users and administrators can safely view suspect messages

Enterprise deployment scenarios

Symantec Brightmail AntiSpam integrates with industry-leading Message Transfer Agents (MTAs) including the Sun Java™ System Messaging Server, Sendmail, Microsoft

Exchange, and Lotus Notes. It has a flexible, modular architecture that allows its components to be deployed on the same or separate servers as needed for availability, reliability, manageability, and security. Indeed, since the product is licensed on a per-user rather than a per-system basis, Information Technology (IT) organizations are free to configure SBAS in the way that best suits their needs

The *Brightmail Client* integrates with the MTA and is responsible for passing e-mail content to and from the *Brightmail Server*, which is the engine that evaluates each message and produces a spam classification based on its content. IT organizations manage the servers across which the components are deployed using the *Brightmail Control Center*. From this secure, Web-based interface with role-based access, authorized administrators can:

- Configure, start, and stop each of the servers
- Specify filtering options for groups of users or for all users at once
- Monitor consolidated reports and logs
- View summary and status information
- Administer the Brightmail Quarantine
- Obtain online help information

Connector components include the *Brightmail Agent*, which communicates with the Brightmail Control Center, and the *Brightmail Conduit*, which communicates with the Brightmail Logistics and Operation Center, retrieving new anti-spam rules as they are created to block new types of spam.

Range of deployment options

Symantec Brightmail AntiSpam can be deployed using a range of architectural approaches. All components (except for the Brightmail Control Center) can be deployed on a single server along with the MTA to protect small businesses. Components also can be deployed in various gateway scenarios, where SBAS integrates with a DMZ-resident MTA, filtering messages before they are forwarded on to internal MTAs responsible for actual message delivery.

SBAS supports round-robin load balancing, enabling the product to be deployed in multiple MTA, high-availability environments. The client can be configured to fail over to secondary or tertiary servers so that an

organization's ability to accept incoming e-mail is not impeded by the failure of one or more of several MTAs.

Such a configuration is illustrated in Figure 2, where incoming e-mail is distributed across three instances of Java System Messaging Server, each of which is integrated with a Brightmail Client. Two Brightmail Servers are deployed so that in the event that one of the servers fails, or must be taken down for maintenance, incoming e-mail can still be evaluated for spam content. The entire operation is managed from a single instance of the Brightmail Control Center.

Coupling SBAS with the Sun Fire T2000 server

The volume of e-mail and spam that an organization must manage is constantly increasing. As spammers use ever more clever tactics to disguise their messages, the processing power needed to maintain high throughput rates must increase apace. Processing e-mail is an inherently multithreaded operation, with servers required

to establish connections with remote MTAs, whether or not they bear legitimate e-mail. Recognizing this fact, Symantec has built SBAS to scan a configurable number of concurrent message streams. With the Sun Fire T2000 server's ability to support a large number of concurrent threads in hardware, Sun and Symantec are made for each other.

The gigahertz race

Most processor vendors have been competing in a gigahertz race, one that seeks to improve performance by increasing processor clock rates. These processors have deep and complex pipelines that must be flushed when a memory request cannot be satisfied from the cache or when the operating system forces a context switch. When a pipeline is flushed, it requires many clock cycles to re-fill the pipeline and do useful work again, wasting both time, power, and generating excess heat. This problem will only get worse as memory speeds increase more slowly than processor speeds and the average amount of time waiting for memory requests to be satisfied becomes ever more dominant in these processors.

The UltraSPARC T1 processor

Sun recognizes that it's not gigahertz, it's *threads* that are the scarce resource for network throughput-oriented software. Unlike traditional single-threaded processors, and even most current multi-core processors, Sun's UltraSPARC T1 processor is designed to support multiple threads per processor core, with the ability to switch between active threads every clock cycle. Sun's Chip Multithreading (CMT) approach enables each processor core to switch among four active threads. When a memory request cannot be satisfied, or a context switch is required, the processor simply switches to another thread while the request is fulfilled in parallel (Figure 3).

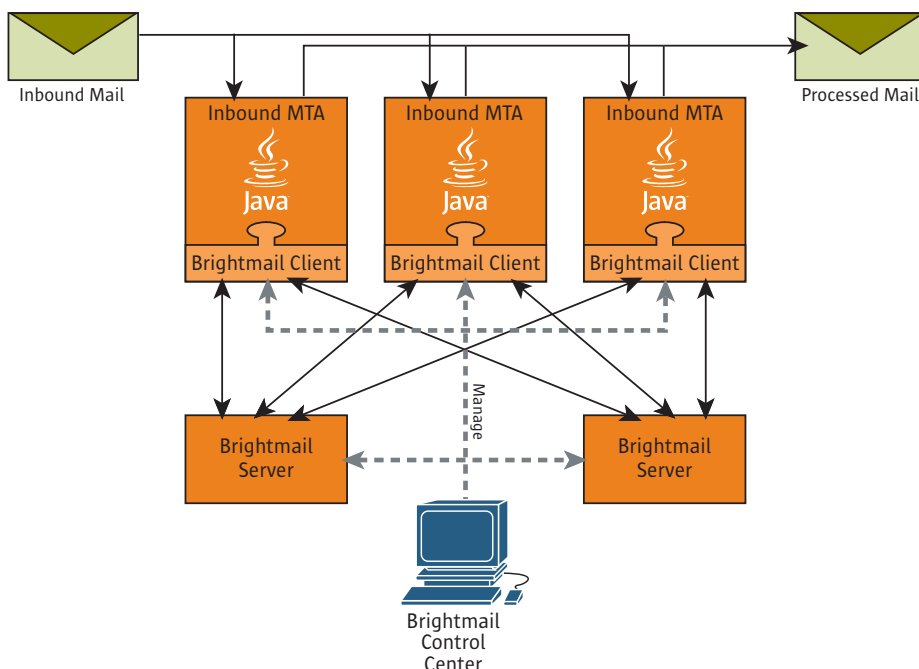


Figure 2. The flexible, modular architecture of Symantec Brightmail AntiSpam allows it to be deployed across multiple servers, as illustrated in this high-availability configuration.

Sun's UltraSPARC T1 processor is available with four, six, or eight processor cores per chip, with

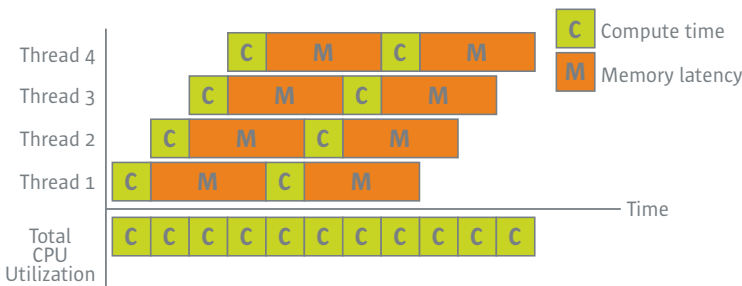


Figure 3. Each UltraSPARC T1 processor core switches between four active threads, doing useful work even as threads stall to perform memory-related operations.

the ability to process 16, 24, or 32 threads in parallel. This makes it perfectly matched for highly multithreaded, network throughput-intensive processing such as that demanded by Symantec Brightmail AntiSpam.

The Sun Fire T2000 Server

The Sun Fire T2000 server is one of Sun's two eco-responsible servers that use space-efficient, rack-optimized designs for data center environments (Figure 4). The Sun Fire T2000 server is available with a single four, six, or eight-core UltraSPARC T1 processor, up to 32 GB of main memory, and up to four 2.5" SAS disk drives with built-in hardware RAID 0 and RAID 1. The server is equipped with four 10/100/1000 Ethernet interfaces. For data center environments, the server features Advanced Lights-Out Management (ALOM) through its own dedicated serial and Ethernet ports. The server includes three PCI-Express expansion slots, and up to two PCI-X slots. Reliability, availability, and serviceability are increased through the use



Figure 4. The Sun Fire T2000 server is built for highly multithreaded workloads

of dual redundant hot-swappable power supplies. Best of all, the Sun Fire T2000 server supports the Solaris™ Operating System, which is optimized for multithreading performance.

Sun and Symantec — Better Together

Not all software is ready to harness the computing power of the UltraSPARC T1 processor out of the box, and Symantec Brightmail AntiSpam is no exception. Sun and Symantec worked together to optimize SBAS performance using a load generator to drive a synthetic workload. The result is a set of tuning steps to increase the number of threads that the software will utilize, and changes to reduce the contention for software locks.

The result is an astonishing 5.2x performance improvement over an initial SBAS installation on a Sun Fire T2000 server with a message-handling rate of 94 messages per second. Given the differences between the test configuration and individual MTA configurations, average message sizes, spam percentages, and the dynamic changes in the filtering rules provided by Symantec, your mileage may vary. Nevertheless, the dramatic 5.2x improvement on the Sun Fire T2000 server, and an 8.2x improvement

Learn More

For more information on the Sun Fire T2000 server, please refer to www.sun.com/t2000.

For more information on Symantec Brightmail AntiSpam, visit Symantec's Web site at www.symantec.com.

For details on how to tune SBAS for maximum performance on the Sun Fire T2000 server, refer to the Sun BluePrints™ article *Tuning Symantec Brightmail AntiSpam on the Sun Fire T2000 Server*, available at www.sun.com/blueprints.

over Sun's own dual-processor Sun Fire V240 server, point customers to the kind of performance improvement that the Sun Fire T2000 server can deliver in comparison to traditional, highly pipelined microprocessor-based servers.

The combination of Symantec Brightmail AntiSpam and the Sun Fire T2000 server is more than a choice of two best-of-breed products. With the two companies working together to optimize SBAS performance, choosing Sun and Symantec is like having a team of experts working to improve your anti-spam effectiveness, accuracy, and throughput.



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com

