Websense Triton Security Gateway Anywhere

A Usability Study and Performance Evaluation

Executive Summary

In today's global economy the ways in which businesses use the Internet have changed dramatically with cloud computing, social networking and burgeoning mobile workforces prime examples of this explosive growth. In turn, these have brought a host of new and highly sophisticated threats to data security which businesses must address if they are to adhere to ever stricter data protection regulations. Many security vendors are also struggling to keep up with the rapid evolution of malware. This has resulted in more complex and costly solutions that are often little more than assortments of third-party products with limited integration.

Websense's latest Triton Security Gateway Anywhere (TSGA) has been developed to address these emerging markets. The company claims this as the first unified content security solution for web, mail and data security that doesn't rely on any third-party content analysis.

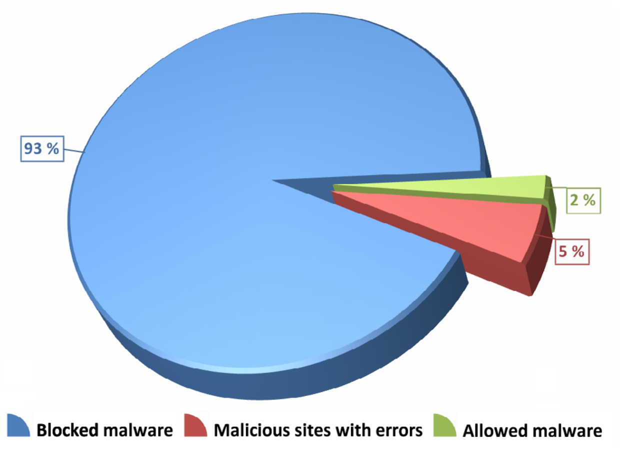
Binary Testing was commissioned by Websense to evaluate the TSGA appliance solution in its lab based in Newhaven, Sussex. Its engineers deployed the appliance in a dedicated test network and looked at ease of use of its unified web interface, integration between the web, mail and data security components, inbound and outbound security policy management and data leakage protection features.

The engineers ran tests using large samples of active web sites harbouring malicious content with a diverse range of attack vectors. Further samples were used of active web sites containing dynamic Web 2.0 content considered to be objectionable. Traffic throughput tests were also performed using a Spirent Avalanche 290 appliance.

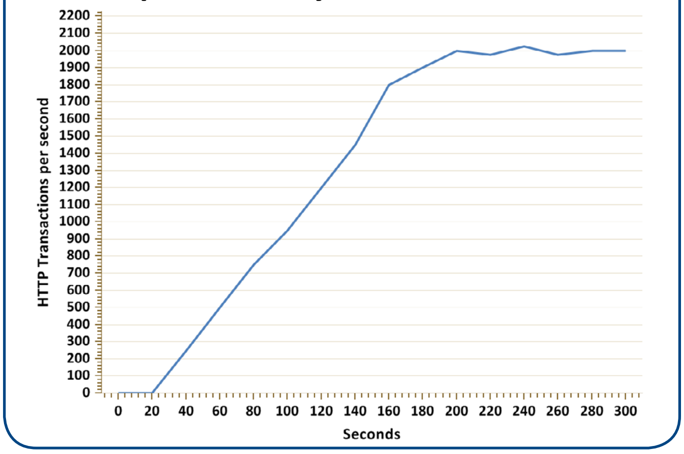
Key Findings

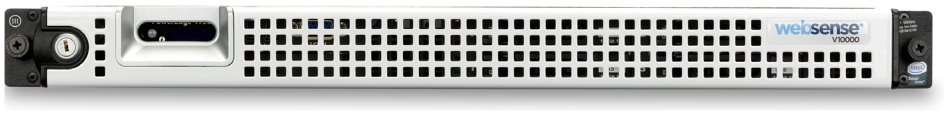
1. Websense TruHybrid is the industry's only security solution to include on-premises scanning and SaaS cloud services
2. All security and reporting features are seamlessly integrated into a single unified management console
3. Offers extensive web, mail and data security measures with sophisticated data leakage prevention
4. Delivers a sustained throughput of 2,000 HTTP transactions per second with all security features enabled
5. Real time categorisation and unified threat analysis deals effectively with dynamic web content and social networking sites

Malware detection accuracy
Sample size - 2,975 malicious web sites



Spirent Analysis of HTTP TPS





Websense's Unified Web Management Interface

The entire TSGA solution is managed from the Unified Security Center (USC) console and the Binary Testing engineers found initial deployment and ongoing administration particularly easy due to its simplified, intuitive design. Websense has avoided any complexity by grouping the main modules under three separate tabs for web, data and email security.

The TSGA Dashboards

Consistency is maintained across each component thus simplifying ongoing configuration and the web and email security tabs both open with customisable dashboards. The dashboards provide clear visibility into all security activities and can be customised easily to show areas of interest such as the current day's detected threats, security risks and policy actions for each module.

The data security component is included as standard and this tab also opens with a dashboard showing a health summary for the day, data loss prevention (DLP) incidents and the most active policies. Further performance and security activity is immediately available from all three tabs. You can quickly bring up historical displays, view alerts or audit logs and, for the web security module, see all activity relevant to the Websense hybrid service.

Policy Creation

Operational consistency has been maintained for policy creation making this a simple process for all three components. The process has been streamlined as existing policies can be used as templates and modified to suit. Each web policy can contain multiple filters and Websense includes one of the most comprehensive URL category lists the Binary Testing engineers have yet seen.

TSGA security policies were found to be simple to create and far more versatile than typical rule based systems. For example, many web security solutions can only enforce URL and protocol filtering as separate, unrelated entities whereas TSGA allows you to combine the two in the same policy.

Websense goes further as bandwidth restrictions can not only be incorporated into the same policy but can have specific values set for individual web categories and protocols. Policy creation for inbound and outbound mail was found to be just as intuitive and DLP policies are even easier to deploy as Websense includes over 1,100 predefined rules as standard.

Multi-Role Management

Management tasks can be delegated by creating various TSGA users each with assigned roles. At the top level, are global security administrators which have super user access to all TSGA modules. Beneath this you can create custom roles where users can be granted monitoring only or full access to any of the web, data or email security modules.

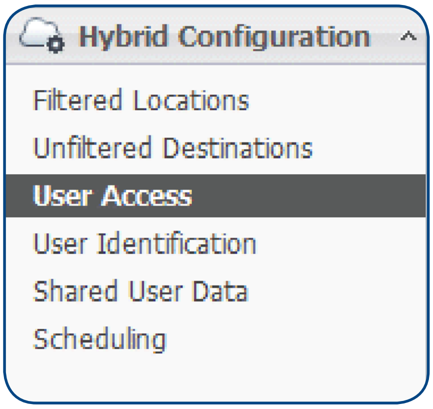
> ***" TSGA security policies were found to be simple to create and far more versatile than typical rule based systems. "***

Reporting Facilities

The Binary testing engineers found TSGA's reporting facilities to be extensive and capable of providing high levels of information. Furthermore, Websense provides sets of predefined reports for each module but allows them to be easily edited to suit requirements.

This is an area many competing solutions fall down on as they often only provide a base set of predefined reports that cannot be modified and rely on customers providing their own third party reporting tools. TSGA reports for all three security modules can be used as templates, saved as new reports, customised extensively and scheduled to run at regular intervals.

Websense TruHybrid Technology



Websense TruHybrid

Websense's TruHybrid technology is unique as it unifies on-premises scanning and SaaS cloud services. It can be deployed for both web and email security and the complete solution managed entirely from a single console.

A key concept is the ability to deploy on-premises web and mail security at the company headquarters and use the SaaS component to extend the same security to branch offices and remote workers.

Competing solutions that offer both services do not have the facilities to manage them from one console. Furthermore, they rely on third party cloud service providers and do not offer any integration between these and the on-premises services.

By unifying these services, TruHybrid allows a single policy to cover both on-site and off-site security. IT support overheads are reduced and all SaaS activity can be reported on using the same TSGA module as for on-site reporting.

How TruHybrid Works

For the web component you can decide precisely which locations and users are to be filtered using the hybrid service. Locations can be defined by IP addresses, ranges or subnets and must be visible on the Internet for the hybrid service to work.

As TruHybrid synchronises the appliances with the cloud services it allows policies created on-site to be applied to remote workers. Consequently, they will have the same levels of security applied to them as their head office co-workers. TruHybrid is highly flexible as user locations can be easily identified by TSGA allowing different web filtering policies to be applied based on whether a user is off-site or on-site.

> ***" Websense's TruHybrid technology is unique as it unifies on-premises scanning and SaaS cloud services. "***

The email component of TruHybrid works in precisely the same manner. The on-premises appliances work directly with the cloud services and determines the most appropriate mail filtering method. Users will then be protected from spam and email threats regardless of their location.

TruHybrid Configuration

The Binary Testing engineers found configuration of the TruHybrid components very simple. The web component has a separate section for TruHybrid configuration where you specify filtered locations along with unfiltered destinations such as company webmail sites that users access directly without going over the Internet.

User connections to the hybrid service can be controlled using PAC (proxy auto-configuration) files or with Group Policies. Either way you can enforce proxy authentication and deliver a custom web blocking page specifically for TruHybrid users. The Websense Directory Agent may also be used to provide the hybrid service with user and group information.

A Sync Service on the appliances communicates with the TruHybrid cloud service and sends it policy configurations and user information gathered by the Directory Agent. It also receives reporting information from the cloud which is amalgamated into the local report databases.

Registering for the TruHybrid email service is equally simple as you decide which email traffic will use the cloud service by defining mail domains and adding DNS details and MX records. On-site and off-site mail security policies are all created from the same user interface.

An important feature of the TruHybrid mail service is its ability to scan mail for viruses, spam, phishing and malware in the cloud. This means that threats are identified and neutralised before they even reach the on-premises appliance so reducing network bandwidth usage and message quarantine storage usage.

Websense Threatseeker Network and ACE

Threatseeker and ACE

The threat landscape has changed dramatically over recent years making signature based security systems ineffective as they can always only ever be reactive. The sheer volume and dynamic nature of threats has increased and include targeted attacks with specific missions which traditional security systems cannot catch.

Websense's ACE (advanced classifications engine) is unique as it provides unified real time deep content analysis for inbound and outbound web, email and data security channels. Included across all Websense products, ACE works with the Websense Threatseeker network to provide high performance analysis of content as it is being viewed.

From a network administrator's perspective, the Binary Testing engineers found that ACE requires no additional configuration after TSGA deployment. Content categorization is enabled by default along with analysis of links embedded within web pages.

Scanning sensitivity is set to the optimum level although this can be modified using a slider bar if required. Outbound traffic will be scanned for bot and spyware phone home activities whilst database updates for the on-premises scanning services are updated at scheduled intervals which can be as often as every 15 minutes.

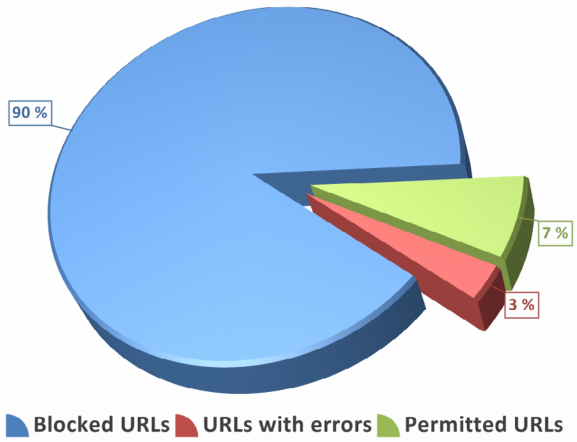
Binary Testing engineers performed inbound threat tests using samples supplied with the Websense URL test kits. These contain web sites harbouring threats such as malicious iFrame redirection, command and control of bot networks and obfuscation using dynamic scripting languages which require real time classification

The test samples provided contain web sites gathered from the Threatseeker database and Websense has no control over them.

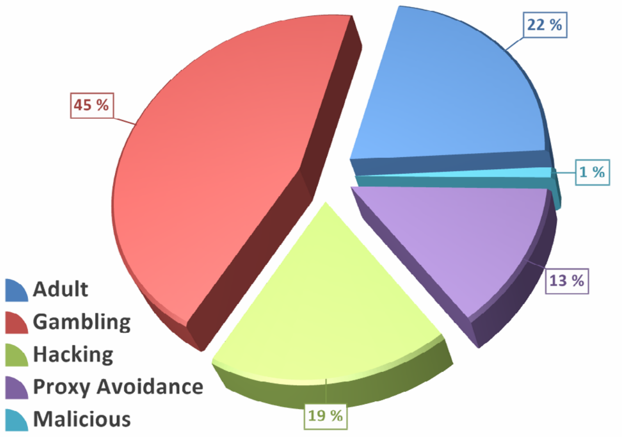
Since the sample was taken, many of the listed web sites may have changed, been taken offline or had malicious content removed or modified to circumvent signature based scanners

This reflects the dynamic nature of the web today and the requirement for the real-time classification capabilities of ACE. In the test results, sites that have been taken offline or cleaned up show as sites with errors or as allowed through.

Dynamic Categorisation - default web policy
Sample size -1,724 URLs



Dynamic Categorisation
Spread of blocked sites



Policy Enforcement and Data Loss Prevention for the Social Web

Social network policy enforcement

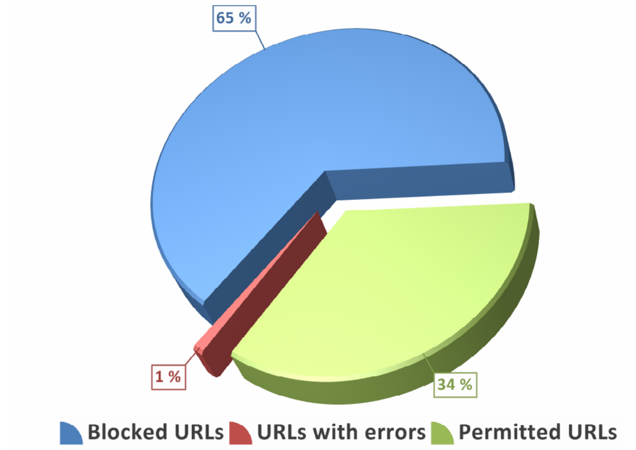
In order to protect data and adhere to regulatory guidelines, businesses must enforce workplace AUPs (acceptable use policies). By providing a unified solution for web, email and data, TSGA simplifies this process as all AUPs can be created, deployed and reported on from a single console. Social networking is also now a major issue as it is fast becoming integral with the way business is conducted.

Sites such as Facebook can be a great business enabler but many also harbour undesirable or unproductive content. Websense's ACE overcomes these issues by examining each page's content so allowing social networking access but in a secure manner.

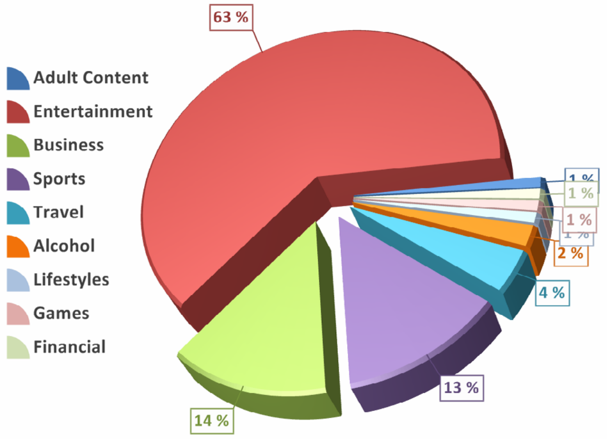
Binary Testing engineers examined these features by using further web site samples from the URL test kit. These contained social networking pages where some were acceptable for business use and others contained undesirable content.

Assuming their URL database was sufficiently up to date, less sophisticated security products would have simply blocked access to every site in the list. As shown in the graphs, TSGA permitted or denied access based on individual page contents.

Dynamic Facebook page categorisation
Sample size - 2,269 URLs



Facebook Categorisation
Spread of blocked sites



Data Leakage Prevention

Websense's data security module provides the facilities to enforce DLP (data loss prevention) policies. For email it can search for patterns and phrases in messages or within attachment content and TSGA includes predefined dictionaries of terms unacceptable for business use.

Regulatory compliancy is very easy to implement as from the console you select which ones you want to apply and choose the country of operation. TSGA determines which regulations are most applicable for your locale and applies them for you.

Fingerprints of sensitive files can be created and even if only a partial match is found the file can be blocked from being sent. Websense's PreciseID identifies content based on a huge dictionary of patterns such as credit card numbers and it can apply image analysis to mail.

The Binary Testing engineers were impressed with the ease with which web and email DLP policies could be created and deployed. Web policies can include size limits on postings, predefined PII, PHI and PCI-DSS regional rules and restrictions on the web sites where sensitive data may be sent.

Mail DLP policies were tested by sending messages across the two mail domains. Some attachments were Word documents with banned content and these were all successfully blocked. Analysis was also tested with a range of images and TSGA was found to be very proficient at quarantining those that were unacceptable.

DLP activity can be monitored closely using a catalogue of predefined reports and views. For blocked mail, the engineers could see these in the incident reports and a forensics window provides views of the entire message content, attachment, recipient and sender.

Websense Application Controls

Application Controls

It’s a well known fact that IM and P2P applications represent significant security risks and yet many vendors pay scant attention to these potential nuisances. Binary Testing has seen many security products that either offer blocking facilities only for a very small range of applications or no controls whatsoever.

Up until now, the only answer to effectively control these applications was to implement costly point solutions. However, TSGA includes protocol filters as standard which provide granular controls for a wide range of applications.

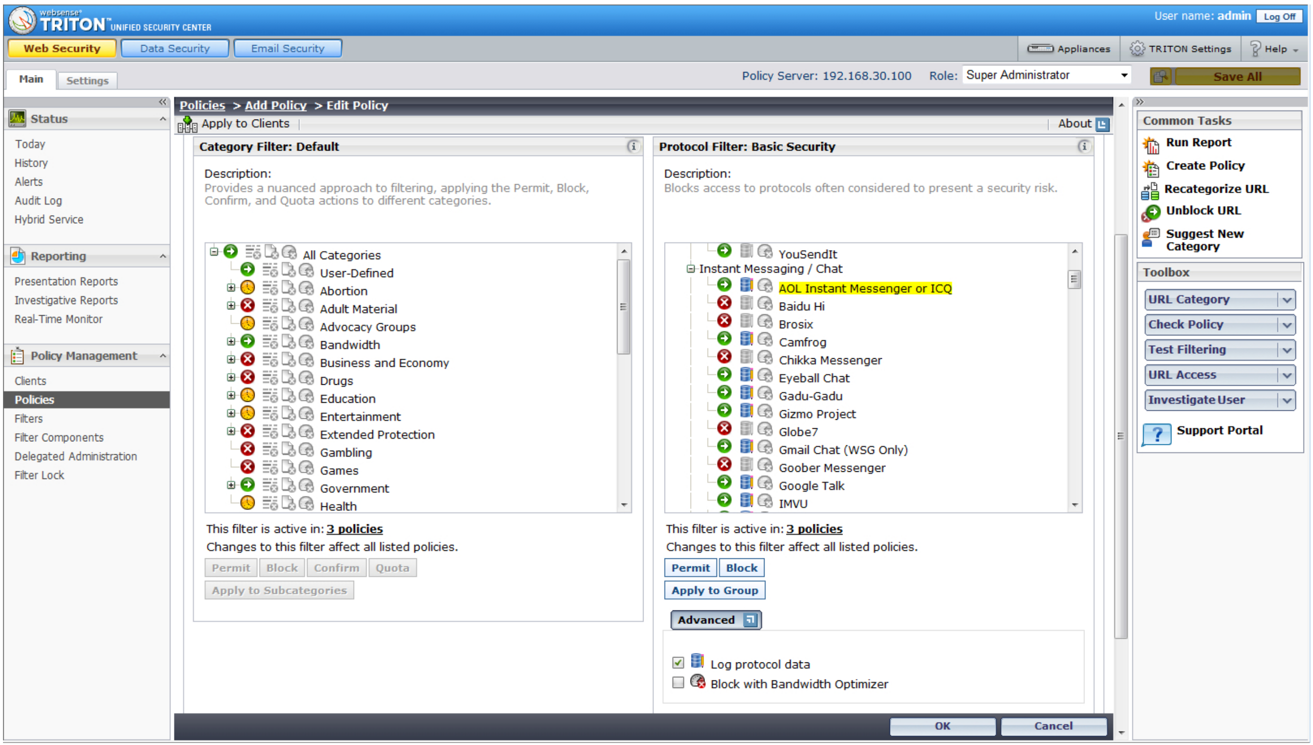
A huge list of predefined applications is provided and includes P2P file sharing and transfer apps, Instant Messaging, media streaming, proxy avoidance sites and many popular remote control tools. During web policy creation you can block or allow each individual application and request that protocol data be logged.

Where certain applications are permitted, you can restrict their impact on the network by applying bandwidth optimisation. This will block further use if utilisation goes above a certain percentage of total network traffic or for this protocol only.

Using protocol analysis allows TSGA to block selected applications regardless of the port being used and whilst Websense’s application list should cover most requirements it is possible to add entries for those using non-standard ports.

We found this a simple process where you add port numbers or ranges and apply IP addresses, ranges or subnets. During this phase it is also possible to activate blocking or allowing actions, data logging and bandwidth optimisation.

The Triton Security Gateway Anywhere unified management console



Policy Server: 192.168.30.100 Role: Super Administrator

Policies > Add Policy > Edit Policy

Category Filter: Default

Description:
Provides a nuanced approach to filtering, applying the Permit, Block, Confirm, and Quota actions to different categories.

- All Categories
  - User-Defined
  - Abortion
  - Adult Material
  - Advocacy Groups
  - Bandwidth
  - Business and Economy
  - Drugs
  - Education
  - Entertainment
  - Extended Protection
  - Gambling
  - Games
  - Government
  - Health

This filter is active in: 3 policies
Changes to this filter affect all listed policies.

Permit | Block | Confirm | Quota
Apply to Subcategories

Protocol Filter: Basic Security

Description:
Blocks access to protocols often considered to present a security risk.

- YouSendIt
- Instant Messaging / Chat
  - AOL Instant Messenger or ICQ
  - Baidu Hi
  - Brosix
  - Camfrog
  - Chikka Messenger
  - Eyeball Chat
  - Gadu-Gadu
  - Gizmo Project
  - Globe7
  - Gmail Chat (WSG Only)
  - Goober Messenger
  - Google Talk
  - IMVU

This filter is active in: 3 policies
Changes to this filter affect all listed policies.

Permit | Block
Apply to Group
Advanced

☑ Log protocol data
☐ Block with Bandwidth Optimizer

The TSGA web console simplifies management immensely by providing full access to all security components from a single, centralised console. In the picture above, we can see the policy creation process and the facilities for blocking web site content and applications.

The V10000 Appliance and Performance Tests

The V10000 Appliance

Many security vendors try to cut costs with their appliances and frequently provide hardware platforms that are underspecified for the task at hand. They may quote a high firewall throughput but this always drops substantially when all UTM features are enabled.

The TSGA V10000 appliance in this evaluation is deployed as a high quality Dell PowerEdge R610 1U rack server. It uses the latest quad-core Xeon processors along with plenty of fast server grade DDR3 memory and includes RAID protected SAS hard disks plus dual redundant power supplies.

The V10000 appliance when deployed with TSGA is aimed at headquarters and large branch office deployments and is designed to run all Security Gateway Anywhere components simultaneously on a single platform. Deployment time is reduced as the appliance is preconfigured and tested prior to being shipped.

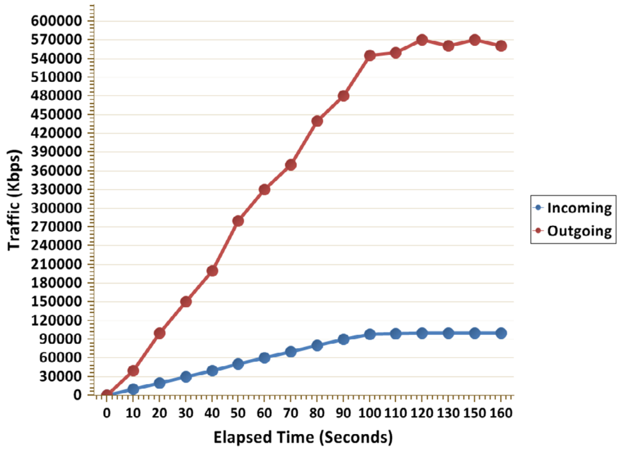
Websense also offers the V5000 appliances which target deployment at branch offices or for medium sized businesses. These are lower cost alternatives to the V10000 and are capable of running any one security component but do not support web and email security together.

Performance Tests

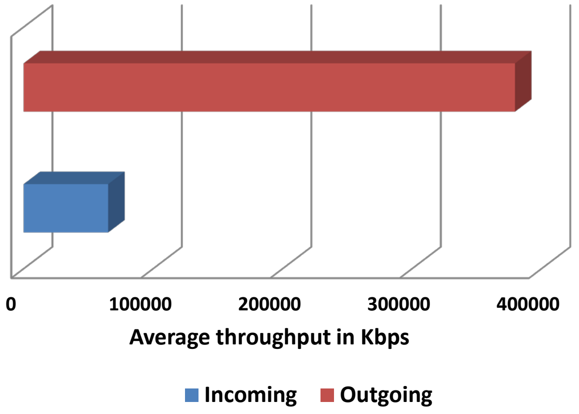
To test performance of the V10000 appliance, the Binary Testing engineers used a Spirent Avalanche 290 appliance. It was connected in 'one-arm' mode to the V10000 appliance over Gigabit Ethernet and tests were conducted with all TSGA security features enabled.

Performance metrics gathered were the maximum sustained HTTP TPS (transactions per second) and maximum inbound and outbound TCP throughput. The Binary Testing engineers also recorded the average TCP response times and successful transactions during these tests.

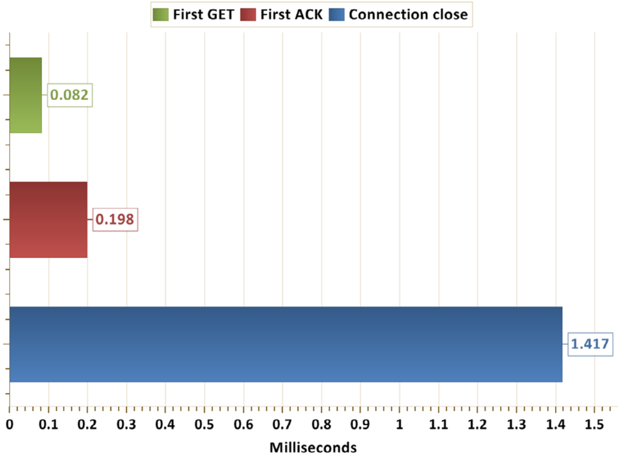
Incoming and outgoing traffic



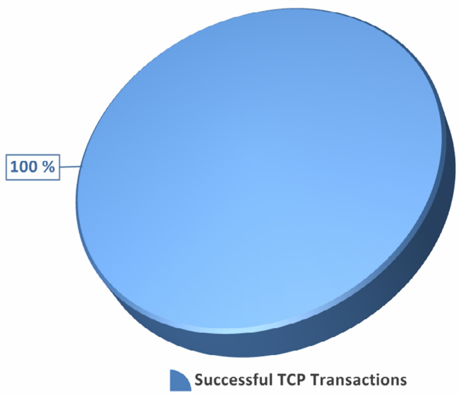
Spirent Avalanche throughput tests with all security scanning enabled



Average TCP response times



Successful TCP transactions



Conclusion and Lab Testing Scenario

The Binary Testing engineers were impressed with the range of web, mail and data security functions Websense has incorporated into the Triton platform. Management using the Unified Security Center (USC) web console is straightforward and all features have been seamlessly integrated into it.

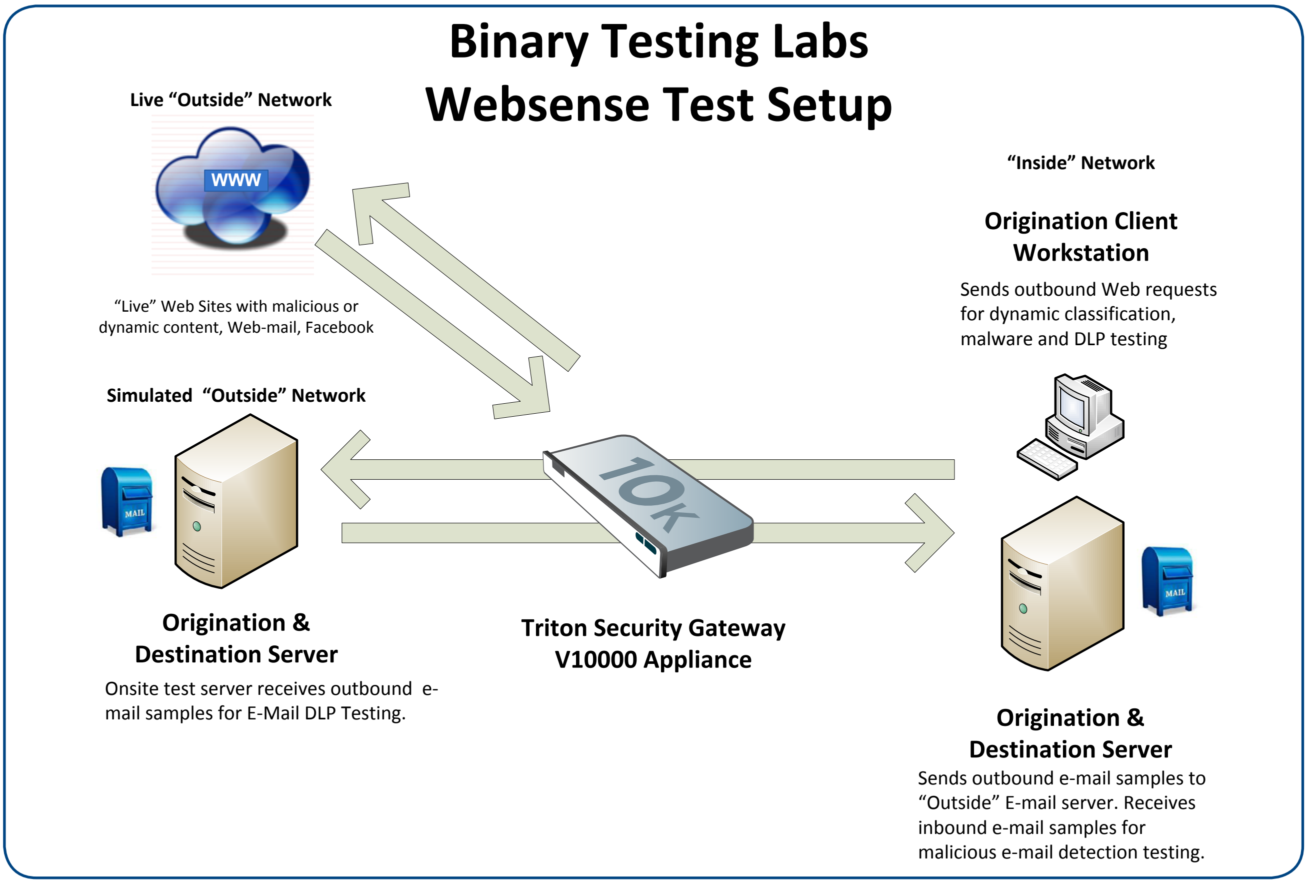
The USC interface was found to be very intuitive and by grouping the main modules under three separate tabs for web, data and email security, Websense has neatly avoided any complexity. The dashboards for each module provide detailed views of all business activity giving a clear insight into all security issues and detected threats.

Policy creation is a swift process and the web security module provides one of the most comprehensive URL category and application lists on the market. DLP (data leakage prevention) policies are very sophisticated and regulatory compliancy can be implemented simply by choose the country of operation from the USC interface.

TSGA when deployed on the V10000 appliance targets organisations up to 2,500 users and performance tests confirmed the appliance is quite capable of handling their demands. With all security features enabled, the Avalanche reported a sustained throughout of 2,000 HTTP TPS at loads up to 440Mbps.

The Avalanche reported no transmission errors whilst TCP responses were also very low. For larger user bases, multiple Triton appliances running different security modules can be deployed to spread the load.

As organisations embrace the Internet, their network frontiers have changed so much that perimeter security is no longer enough. Websense's Triton Security Gateway Anywhere represents the next generation of business security solutions and along with a remarkable range of features, succeeds in seamlessly integrating both on-premises and SaaS cloud services into a single unified platform.



Binary Testing Labs
Websense Test Setup

Live "Outside" Network
WWW
"Live" Web Sites with malicious or dynamic content, Web-mail, Facebook
Simulated "Outside" Network
MAIL
10k
"Inside" Network
MAIL

Origination Client Workstation

Sends outbound Web requests for dynamic classification, malware and DLP testing

Origination & Destination Server

Onsite test server receives outbound e-mail samples for E-Mail DLP Testing.

Triton Security Gateway V10000 Appliance

Origination & Destination Server

Sends outbound e-mail samples to "Outside" E-mail server. Receives inbound e-mail samples for malicious e-mail detection testing.