



Secure and Manage  
Your Internet Access



## Anchiva Secure Web Gateway

### Overview

#### Risks and Challenges Confronted Enterprises in the Internet Era

With the development of web technology, more and more internet applications come into being, enabling people to access a vast range of knowledge, exchange messages, empowering businesses to create more opportunities, promote rapid expansion and become more competitive.

However, internet access in the workplace also increases the risks of attacks from hackers attempting to break into the network, and planting malwares such as virus, Trojan horse, spyware, worms. These malwares infect computers, destroy data, steal sensitive information for economic purpose, and even trick user PCs into a bot, which has been a growing trend among internet attacks. According to a Garner's report, 75% corporations were infected by undetected malwares with economic purpose which can evade traditional peripheral and host defense software.

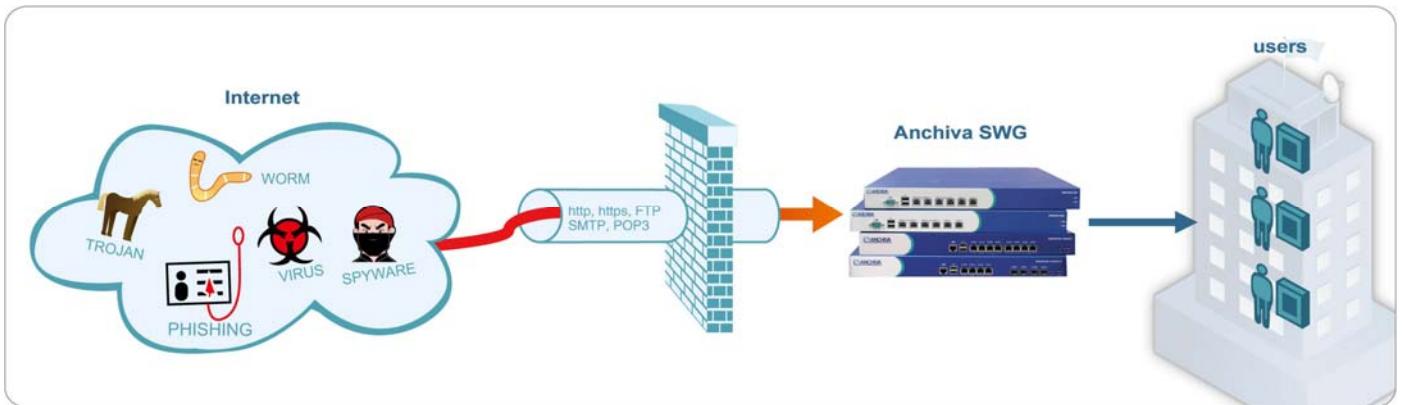
Besides, internet access makes it possible for employees to abuse the network with IM, e-commerce, online gaming, online stock trading, online TV/ streaming media, and web downloading tools like BT during work hours. These activities may greatly affect productivity, cause internet traffic jam, and even leak sensitive information and bring legal liability to the company with inappropriate utterance on the web.

#### Anchiva Solutions

How to resolve these internet threats and problems, how to optimize resources, improve productivity, and reduce bandwidth cost, prevent data loss and avoid legal liability has been a common concern to all enterprises. Anchiva's Secure Web Gateways offer IT staff a single platform to manage and control multiple key security features: anti-malware protection, URL filtering, internet application control, bandwidth management and web application firewall, providing a better solution in internet application security and management:

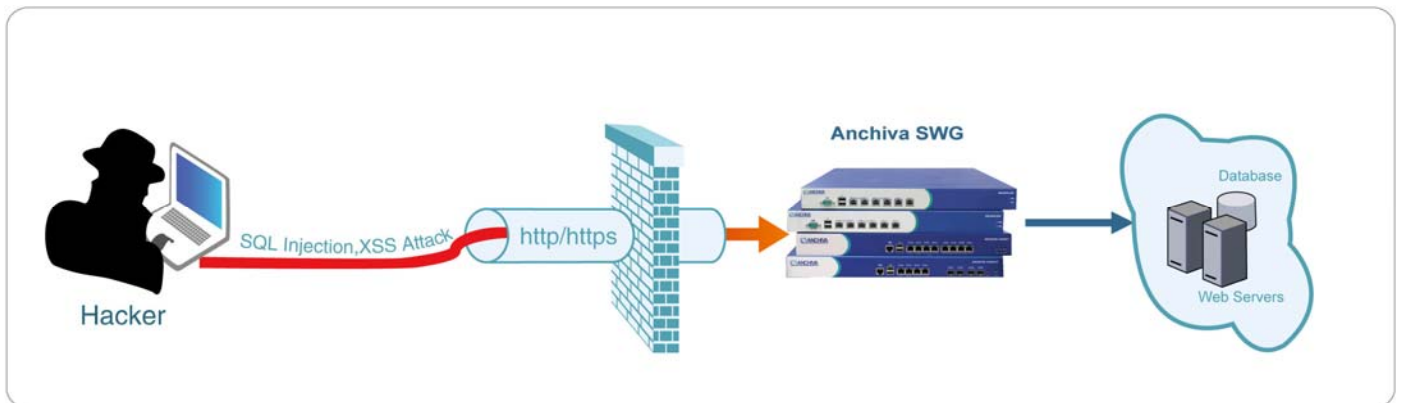


- **Protect enterprise networks against malicious attacks from Internet and Intranet to ensure the security and reliability of network.**



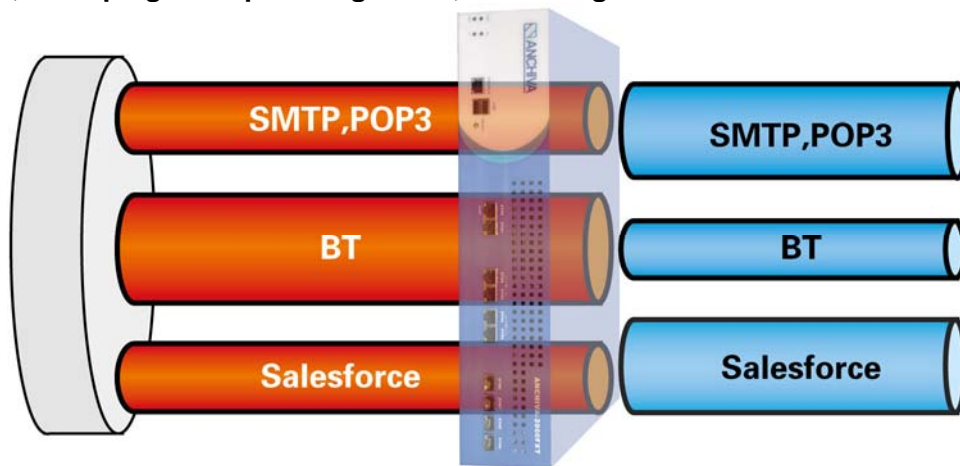
**Value proposition:** prevent attacks from virus, Trojan, spyware, and botnet.

- **Protect enterprise web servers from malicious attacks which may cause financial loss and reputation degrading.**



**Value proposition:** prevent web servers breakdown, data manipulation or tampering caused by attacks.

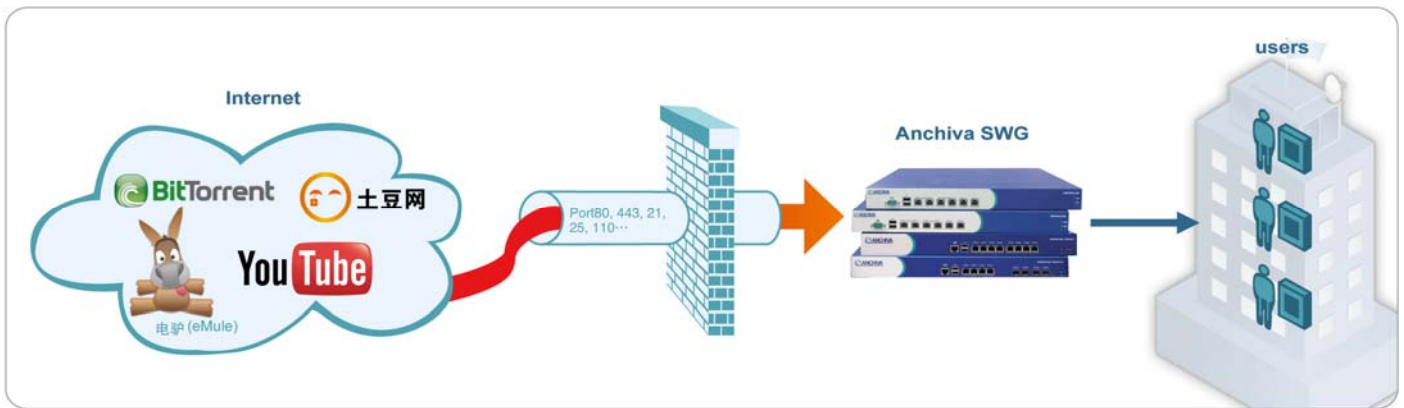
- **Guarantee bandwidth for mission-critical applications and limit volume of non-productive applications, reshaping and optimizing traffic, enhancing business effectiveness and productivity.**



**Value proposition:** optimize bandwidth usage and improve poor performance of key business applications.

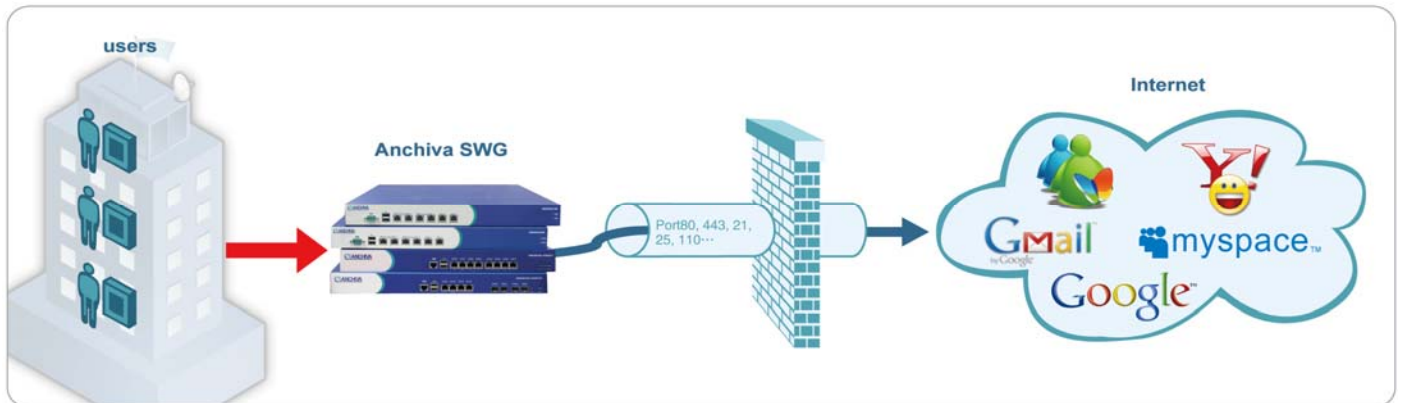


- Control and manage use of downloading tools (BT) and streaming media to realize effective bandwidth allocation and traffic control, increase utilization and save costs.



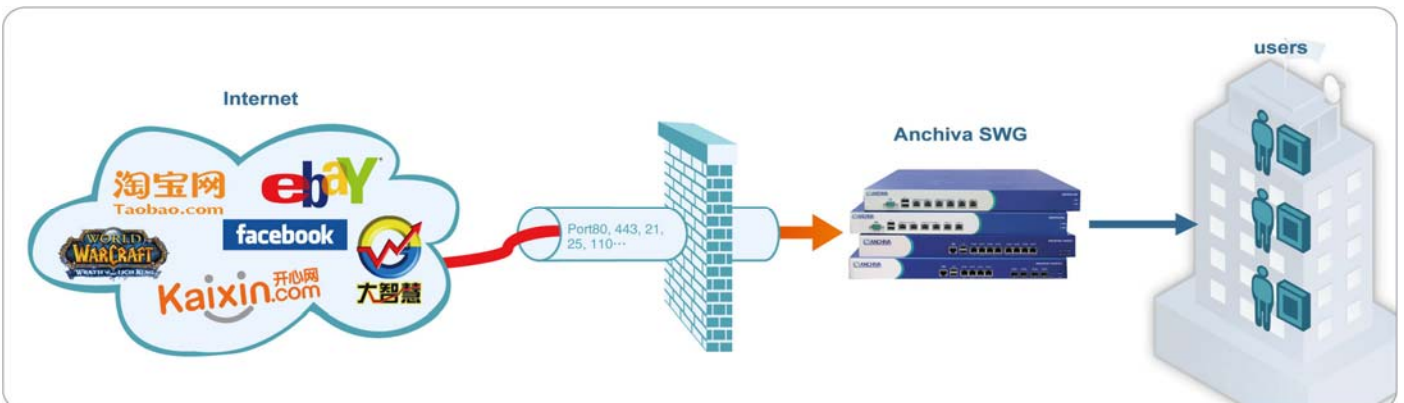
**Value proposition:** effectively manage downloading tools (BT) and streaming media.

- Provide audit on IM (MSN, Yahoo) content. Support key word filtering on webmail text and attachments, BBS posts, and web searching, to prevent leakage of corporate confidential information.



**Value proposition:** prevent confidential information leakage.

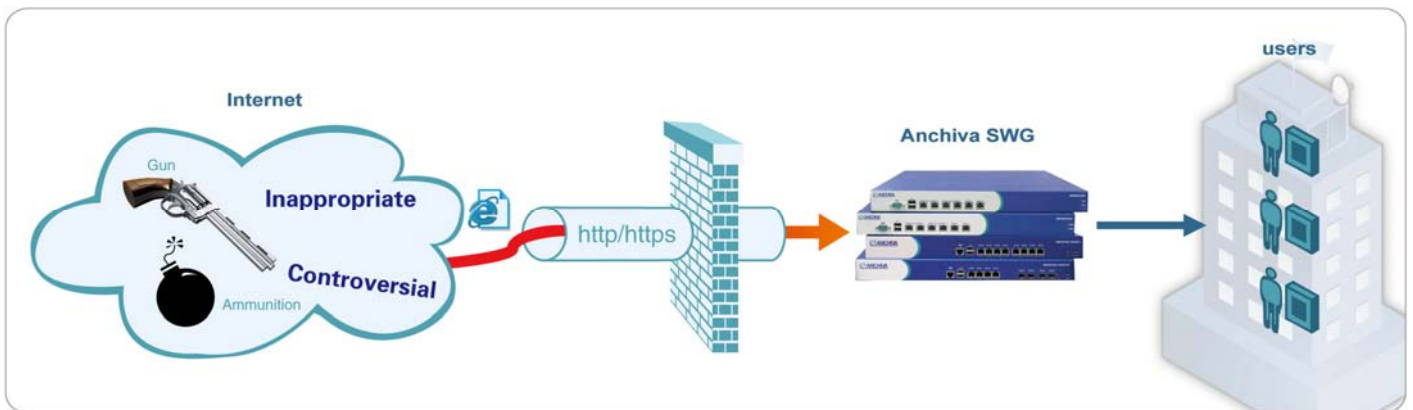
- Prevent employee access to IM, e-commerce, online gaming, online stock trading, and internet surfing. Improve productivity by managing employee internet access.



**Value proposition:** prevent abusive non-productive applications such as IM, e-commerce, online gaming, and online stock trading during working hours.



- Prevent employee access to illegal websites, distributing illicit utterance, so as to avoid negative impact caused by employee’s inappropriate behavior.



**Value Proposition:** prevent inappropriate content entering enterprise network.

**Product Features**

**Anti-malware**

Leveraging *Malicious Sites Filter, Deep Content Inspection(DCI) and Signature Matching Engine, Heuristic Engine*, Anchiva Secure Web Gateways provide scanning and filtering on inbound and outbound internet traffic of HTTP, HTTPS, FTP, SMTP, POP3, SMTP in real-time to the maximum extent, ensuring the accuracy and at the same time decreasing the misreport. Major features include:

- Analyze, inspect and block web threats like virus, Trojan horses, worm, backdoor from two-way traffic of HTTP, HTTPS, FTP, SMTP, and POP3.
- Prevent spyware call home
- Filter and block malware origin
- Prevent phishing
- Filter malware downloaded in multiple packets
- Provide zero-day attacks protection
- Timely identify infected internal hosts to prevent outbreaks
- Filter and block botnet web servers

**Anchiva RapidRX Labs provides updates up to 6 times daily.**

**Bandwidth management**

Anchiva SWG provides detailed bandwidth statistics on Web-based applications and user traffic that enhance the transparency of the enterprise network and help administrators understand the overall network bandwidth usage, and thus facilitate the implementation of bandwidth control policies based on Web applications, users and time range.

Web-based applications, URL categories, IP/IP group/ IP address segment, the user/user group, time period of the uplink traffic and downlink traffic bandwidth guarantee as well as bandwidth limitations, not only can provide control and limit speed on non-critical applications to reshape traffic, but also be able to provide bandwidth guarantees and application acceleration for critical business systems or Web applications.

**Support user define protocol and URL category. Provide constant signature customization and upgrading services.**



**Product  
Features****Internet Application Control**

Anchiva SWG provides granular controls based on user and time period, which allows, blocks, or limits access to internet applications such as IM, P2P, streaming media, online gaming, and online stock trading and other web applications. Full logging and reporting capabilities give IT staff detailed information on internet use. Furthermore, the flexibility of the SWG policy engine allows exempt rules and policies to be put in place for privileged IP or staff.

**Provide customized application signature library updates continuously.**

**URL Filtering**

The Anchiva SWG utilizes Data Cloud URL filtering technology. With more than 60 website categories, heuristic collection and classification platforms in the "cloud", Anchiva SWG decreases the risk of productivity loss caused by employee's access to Instant Messaging, financing, e-commerce, and entertainment sites; reduces bandwidth loss owing to web downloading, streaming, and P2P; minimizes legal liabilities caused by accessing drug and criminal sites. Furthermore, URL filtering can block malware infected sites, phishing and botnet sites, so as to eliminate network threats and reinforce a safer network.

**Cloud computing technology provides URL category updates in real time.**

**Web Application Firewall**

Anchiva Web Application Firewall is deployed in front of Web servers to provide real-time scanning, inspecting and filtering to http/https protocol traffic before they go through the web servers. In this process malicious content and activities are blocked from accessing web servers and executing unauthorized operations. Anchiva Web Application Firewall is designed to face the challenges of Web 2.0, providing proactive protections rather than recover the damage after attacks. It gives consolidated protection against malicious code, illegal webpage alteration, and application-targeted attacks. Anchiva Web Application Firewall can prevent: webpage content distortion, website data leakage, password break-ins, and system administrator authority leaking. It prevents infection of Trojan, virus, malicious code, and spyware. It guards user input data and user account, and stops SQL injection, XSS attack and controls Web crawler. Features include:

- **Deep analysis on HTTP/HTTPS protocols**  
Conduct deep analysis on HTTP/HTTPS protocols, exam all fields such as cookie, get parameters, and post forms and decode them if needed to inspect the original content for malicious content.
- **Proprietary signature database**  
The attack signature database is the most core content of Anchiva Web Application Firewall. Anchiva web security researchers extract attacking signatures from a large amount of samples of all types of web attacks. As new types of attacks appear, new signatures will be extracted and database will get updated and sent to users through automatic upgrade networks.
- **Support user defined policy**  
Besides Anchiva attack signature database, users are free to define policy according to specific website by setting rule to block unauthorized access.

**Signature database is maintained professionally by Anchiva RapidRX Security Center with no technical knowledge requirement from users.**



**Anchiva  
Difference****All-purposed Appliance**

Anchiva provides customers several internet application security and management solutions by integrating multiple functions into a single appliance. Customers hereby are free from the headache of assembling and configuring various products for a number of functions. The all-in-one Anchiva SWG solves the problems of having their Internet access protected, application controlled and managed while reducing their investment on capital expense.

**High Performance Platform**

Patented technology in ASIC accelerator and ASIC accelerated scanning technology, AnchivaOS with optimized TCP protocol stack supporting latest multi-kernel hardware platform, make up the basis of Anchiva SWG's high performance. This console has broken the performance bottleneck of common security network appliances, and provides customers a high performance platform that can grow in linear fashion with the hardware upgrade in the future. Anchiva SWG passed the ICSA performance test in 2007 and has proven its leadership in high performance.

**Worldwide Distributed RapidRX Security Labs**

Anchiva has its own RapidRx Security Labs with researchers in North America, Europe and Asia-Pacific, engaging other top notched network threat analysts and researchers around the world. Anchiva possess collecting network, threat processing center, and threat scanning and inspecting technology, and the ASDN provides 24-hour's upgrading services to ensure user networks are protected by latest technology. In response to harmful virus outbreaks, Anchiva can provide solution within two hours to provide customers zero-day protection.

**Largest Onboard Anti-malware Signature Database**

Anchiva's proprietary malware signature conversion technology makes Malware signature identifiable by ASIC accelerator, and by storing the signatures into ASIC high-speed storage unit making them upgradable resolves the problem of ASIC'S inability to upgrade. Anchiva SWG detect and block over 10 million epidemic malware on normal payload.

**ICSA Anti-virus Certified**

Anchiva's malware detection engine is certified by ICSA monthly to ensure Anchiva Secure Web Gateway has 100% detection rate and can prevent the latest malware threats on the internet. Comprehensive testing is performed monthly on the Anchiva SWG by ICSA with approved results.

**Fine Network Adaptability**

AnchivaOS's dedicated session tracking engine and policy engine tracks the source and destination of each session and their routing information, setting the foundation of its interoperability such that Anchiva SWG can be deployed easily in the layer 2 bridge mode with VLANs, or layer 3 routed mode, and even single arm routing topology. Additionally, its configuration is simple with no need to change the customer's existing network.

**Flexible Deployment**

Anchiva secure web gateways support both inline and Port Span monitoring deployment modes in inspecting, blocking and managing internet applications. It behaves as a layer two device in the network topology without any change in existing IP assignment and management policy.





**Product Line**

**Note:**

1. \*Suggest PCs: Is from substantial practical experience of deployment cases in Anchiva customer networks, for reference to evaluating anti-malware feature.
2. \*HTTP Throughput 1: Test based on connecting to www.google.com home page, for reference to evaluating anti-malware feature.
3. \*HTTP Throughput 2: Test based on transmitting Windows notepad.exe file, for reference to evaluating anti-malware feature.
4. \*HTTP Max Concurrent Sessions: Tested based on 64bytes text/html file, for reference to evaluating WAF and URL Filtering features.
5. \*HTTP New Sessions/Second: Test based on 64bytes text/html file, for reference to evaluating WAF and URL Filtering features.
6. \*UDP Throughput (one way): Tested on based on RFC2544, for reference to evaluating Bandwidth Management feature.
7. 1060FT,2000FXT Support Fiber Interface Bypass.

**Typical Clients**



Anchiva System Ltd.  
2033 Gateway Place 5th Floor, San Jose, CA 95110  
Phone: +1-408-392-2300, Email: info\_us@anchiva.com  
**For more information, visit** [www.anchiva.com](http://www.anchiva.com).

**Product Quality Control and Services**

Anchiva Services provides a wide range of service available for purchasing. We strongly recommend that you purchase the continued service to assure the latest software version and user experience. In addition, Anchiva provides professional consulting services, installation services and configuration support as well as corresponding training courses.

All information referred in this document may be updated at any time, and Anchiva will not notify especially. Copyright ©2009 Anchiva System Ltd. All rights reserved. AnchivaOS and Anchiva are registered trademarks. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.