EVOLVE TECHNOLOGY GROUP

BID RECEIVED LATE
Buyer Connie Barnard
Witness
DISQUALIFIED

Technical Response

Presented to:

West Virginia Department of EDUCATION

06/13/13 02:50:56 PM
West Virginia Purchasing Division

Property	Description
Customer and Contact	**Connie Oswald** West Virginia Department of Administration Purchasing Division 2019 Washington Street, East P.O. Box 50130 Charleston, WV 25305 F: 304-558-3970 connie.s.oswald@wv.gov
Document Name	**Proposed Solution to West Virginia Department of Education RFP for Internet Filtering and Reporting Project**
Document Author and Contact Information	Anthony Lange 916-295-1563 alange@go-evolve.com 233 Technology Way, Ste. 4 Rocklin, CA 95765
Creation Date	June 13, 2013

Table of Contents

Ms. Connie Oswald
West Virginia Department of Administration
Purchasing Division
2019 Washington Street, East
P.O. Box 50130
Charleston, WV 25305

June 13, 2013

Dear Ms. Oswald,

Thank you for the opportunity to respond to the attached RFP. Evolve Technology Group is committed to delivering the best security at the lowest total cost of ownership (TCO) to protect organizations against modern threats. Websense security solutions will help you maintain business workflows and operate in new, more efficient, and innovative ways.

Evolve Technology Group would like to propose Websense® Web Security solutions to meet your business requirements. Websense Web Security protects your network and resources against the latest threats. It's informed by real-time security updates provided by the Websense ThreatSeeker™ Network, a collection of more than 900 million unified endpoints that uses the security defenses of Websense ACE (Advanced Classification Engine) to analyze 3-5 billion requests per day.
Websense Web Security solutions offer these features:

- **Best protection without a proxy:** Security intelligence from the ThreatSeeker Network and real-time security updates for the latest protection and ratings;
- **Reduced complexity:** Transparent deployment using existing network infrastructure and One user interface to manage Web Security and any additional Websense email, data or mobile security product;
- **Improved protection:** Reduce malware infections and the risks of data theft and damage to reputation;
- **Intuitive management and reporting:** Set of four customizable dashboards for a comprehensive view into network activity and threat levels, and easy customization, generation and distribution of reports.

The following response to your RFP will demonstrate how Websense can meet your requirements. We look forward to having further discussions with you as you move on to the next phase of your project. Please feel free to contact me at 916-295-1563 or alange@go-evolve.com should you require any additional information.
Sincerely,

Anthony Lange
Senior Account Manager
Evolve Technology Group
233 Technology Way, Ste. 4
Rocklin, CA, 95765

Project Objective:

Evolve Technology Group is an enterprise value added reseller. Evolve Technology Group's mission is to provide comprehensive technology solutions that drive efficiencies into the datacenter. Through the use of technology, we strive to save you time and money. Our goal is to architect the right combination of products and services and to leverage our years of experience in helping our customer succeed in the world of IT.

For over 10 years, Evolve Technology Group has been designing, implementing and training on Websense solutions. As one of Websense's Enterprise Alliance Partners (EAP), Platinum level authorized and Certified Triton Integrators (CTI), we have established ourselves as one of their premier partners in the U.S. We have the highest levels of certifications for our Websense Certified Engineers and are a trusted partner to Websense.

Our project objective is to provide enterprise class web security and reporting to the West Virginia Department of Education. We will provide this solution in partnership with Websense. Websense is the leader in Web, Data, and Email security.

Websense Company Background

Overview

Websense, Inc. (NASDAQ: WBSN), a global leader in unified Web, data, and email content security, delivers the best security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market, and small organizations around the world. Websense is distributed through a global network of channel partners and delivered as software, appliances, and Security-as-a-Service (SaaS). Websense unified content security helps organizations take advantage of powerful new communication, collaboration, and social Web business tools while protecting from advanced persistent threats, preventing the loss of confidential information, and enforcing Internet use and security policies. Websense is headquartered in San Diego, California, with offices around the world.

Websense Management Profiles: http://investor.websense.com/management.cfm

Corporate Governance Information: http://investor.websense.com/governance.cfm

Research and Development

Websense maintains R&D facilities in San Diego and Los Gatos, CA; Reading, England; Sydney, Australia; Ra'anana, Israel; and Beijing, China. With hundreds of R&D employees, the Websense research and development department includes content operations, security research, software development, quality assurance, and documentation.

Websense Security Labs™ drives security research and discovers, investigates, and reports on advanced threats that traditional security research methods do not capture. Recognized as a world leader in security research, Websense Security Labs publishes findings to hundreds of security partners, vendors, media outlets, military, and other organizations around the world 24 hours a day, 7 days a week on the award-winning Websense Security Labs blog. With a team of global threat experts and operations in the Americas, Europe, Middle East, Africa, and Asia Pacific, Websense Security Labs continuously monitors threats including Internet-borne threats and those that stem from web, email, instant messaging, and peer-to-peer file-sharing.

Technology

The company's flagship Websense TRITON solution offers unified web security, email security, mobile security, and data security solutions together or individually. The TRITON solution is available in enterprise-grade appliances, as cloud-based services, and as powerful and efficient hybrids of on-premise and cloud elements working together. No other vendor offers a similar level of security effectiveness and ease of deployment and use.

The proven security effectiveness of the Websense TRITON architecture is based on ACE (the Advanced Classification Engine). Real-time inline contextual defenses within ACE use security, data, and content classifiers that adjust dynamically, based on composite risk scoring, for the most effective security available. Security intelligence and analytics in ACE come from the Websense ThreatSeeker Network, which unites more than 850 million endpoints and analyzes 3-5 billion requests per day from social networks, websites, and email. The Websense ThreatSeeker Network's adaptive security cloud technology uses more than 50 million real-time data-collecting systems that continuously monitor

internet content — including new and dynamic content — for emerging threats. As a result, Websense can adapt to the rapidly changing internet at speeds not possible with traditional security and basic filtering solutions.

People and Places

Websense has more than 1,400 employees worldwide and 26 offices with major development centers in China, the United Kingdom, and Israel. The company also has 173 patents granted and pending in the U.S. and internationally, and has achieved Service Capability & Performance (SCP) certification for world-class customer support.

Contact Us: https://www.websense.com/Content/contact-us.aspx

Websense Product Overview

In 2009, Websense increased its lead in protecting customers from modern Web-based and blended threats by introducing:

- The Websense V10000™ secure Web gateway appliance, a tightly integrated hardware/software platform that leverages the Websense TRITON Advanced Classification Engine of the ThreatSeeker Network to identify and mitigate Web-based threats "on-the-fly" in customer environments.
- The Websense ThreatSeeker Cloud, a cloud-based security service for third-party solution providers that allows managed service providers and other partners to deliver Websense dynamic security protection to their customers.
- Defensio™ Web service, a cloud-based Web 2.0 security offering that filters malicious code and comment spam. The Defensio service, which is available for Facebook subscribers as well as other Web 2.0 users, protects tens of thousands of personal Web 2.0 sites. The visibility Defensio provides into the dynamic user-generated Web provides an early threat detection system that enhances the ThreatSeeker Network.

In addition to enhancing Websense Web security offerings, Websense continued to make strides in integrating the functionality of Web, Email, and Data security solutions. Websense believes that unifying these technologies in a single architecture provides superior protection for customers and significant competitive advantage. This has been the guiding principle of the Websense product development program, and in early 2010 achieved a significant milestone with the introduction of the Websense TRITON solution.

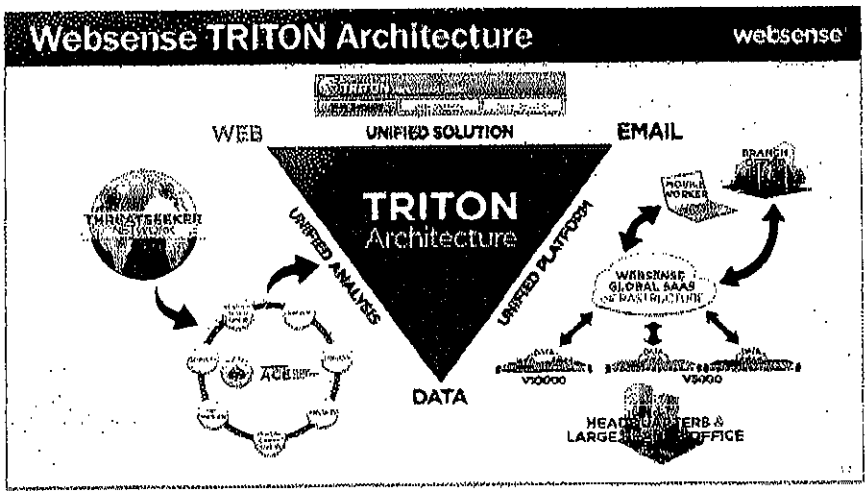
The result of three years of focused development efforts, the TRITON solution leverages real-time security technology and achieves multiple industry firsts, including:

- Administration of Web, Email, and Data security policies from a single management console.
- Delivery of modern security with Websense TruContent™ intelligence — unifying content visibility and analysis to the data level as it flows in and out of an organization, including TruWeb DLP™ and TruEmail DLP™ technologies.

- Seamless integration of on-premise and SaaS implementations through the Websense TruHybrid™ deployment solutions for maximum flexibility and lower total cost of ownership.
- Integrated management reporting and event alerting.

TRITON Solution

Websense helps organizations protect their essential information through the industry's first and only unified content security solution for the global office. The Websense TRITON solution combines Websense market-leading Web, email, and data security technologies into one, unified solution that safely enables use of the social Web and cloud computing, prevents data loss, and extends coverage to the branch office and mobile worker.



The resulting combination of Websense technologies offers these unique and effective security capabilities:

- **Unified Analysis:** The TRITON solution delivers real-time protection against blended and emerging threats — no matter where they reside — through its unified content analysis. You avoid the cost and complexity of point security solutions and the gaps left by legacy products. You also gain enhanced regulatory compliance capabilities and can benefit from new, Web-based communication and collaboration tools.
- **Unified Platform:** A modern enterprise network infrastructure extends far beyond a single location to branch offices and mobile workers. The TRITON solution addresses this challenge with a unified platform consisting of hybrid deployment that integrates both cloud-based and on-premise platforms. This unified platform enables you to better manage risk, further reduce complexity, take full advantage of existing infrastructure, and eliminate management overhead.
- **Unified Management:** The TRITON solution also combines the management and reporting capabilities for Websense Web, email, and data loss prevention technologies into a single interface. Unlike solutions based on disparate products that rely on overlapping or duplicate multivendor management tools, the TRITON solution gives you superior control of your security through a single console.

Only Websense consolidates security to deliver the best security for modern threats at the lowest total cost of ownership. A single unified solution addressing West Virginia Department of Education requirements will significantly reduce the Total Cost of Ownership in a number of ways, including, but not limited to, license, support, and hardware cost savings.

Websense Web Security

Web Security blocks web threats to reduce malware infections, decrease help desk incidents and free up valuable IT resources. With more than 100 security and filtering categories, hundreds of web application and protocol controls, and 60-plus reports with customization and role-based access, Web Security is an easy to deploy and transparent solution that avoids the complexity of a proxy gateway.

Real-Time Security Updates and Granular Policy Controls

- Receives real-time security updates from the ThreatSeeker Network. It's one of the world's largest threat analysis networks, and includes input from Facebook.
- Includes industry-leading web security policy controls, more than 100 web security and content categories, and time quotas with multiple authentication options for users and groups.
- Custom allow/deny filters can be timed or permanent, and can accept security intelligence from third-party sources.
- Has controls addressing viral, entertainment and surveillance videos, plus support for YouTube educational videos.
- Websense Network Agent provides hundreds of controls for applications and protocols, and full port monitoring outside of proxy analysis.

Unified Management and Reporting

- The Websense TRITON Unified Security Center simplifies provisioning and enables role-based reporting.
- Includes more than 60 predefined reports, many easily customizable reports and administrative alerts.
- TRITON architecture supports expansion to email, data or mobile security products, or upgrade to Websense Web Security Gateway.

General Requirements

The products and services that are bid must be capable of providing a level of service appropriate for Internet Service Provider (ISP) facilities with 10 gigabits of Internet bandwidth. School based or district based filtering solutions are not an acceptable response to this RFQ.

Websense Web Security (WWS) can be scaled up to 10Gbps of traffic.

The WVDE currently has two independent Internet connections for the K-12 public schools. Internet filtering solutions must be installed at both Points of Presence (POP).

Websense Web Security can be deployed at both of your POP sites.

Because of the diverse needs of schools, the WVDE must have selective filtering levels and capabilities for delegated administration of tailored filtering policies or profiles for different sub nets.

We do offer delegated administration of filtering policies and reporting.

Updates to the filtering solution must be provided at least once each day to ensure that the filtering database is up-to-date using multiple methods and resources for the review of content on Internet sites.

Websense Web Security leverages our Real-Time Security Updates (RTSU) technology which is capable of pushing out database updates to you every five minutes to provide you the most up-to-date protection against the latest harmful sites.

The Internet filtering must meet the requirements of the E-rate program (refer to http://www.usac.org/sl0 and the West Virginia Board of Education Policy 2460 that is available online at http://wvde.state.wv.us/policies/policy.php?p=2460&alt=1. Information relevant to the Children's Internet Protection Act (CIPA) and the Federal requirement to implement Internet filtering is detailed at the URL http://www.fcc.gov/cgb/consumerfacts/cipa.html.

Websense meets the requirements of the E-rate program. Websense helps schools comply with CIPA by offering the following controls in our WWS product:

- **Obscenity and Pornography Filtering:** Allows schools and libraries to manage Internet access to over 90 URL categories including Racism and Hate, Adult Material, Hacking and other topics pertinent to CIPA;
- **Best-of-Breed Web Filtering:** The most accurate and up-to-date filtering database with over 36 million URLs;
- **Filtering of Search Engine Images:** Use safe-search to filter inappropriate images that can be found in search engine query results;
- **Blocking of Spyware, Malicious Mobile Code, and Other Security Threats:** Sites with worms, spyware, phishing, and other threats can be blocked, helping to meet The CIPA requirements for protection of a minor's personal information;
- **Monitoring:** Reporting Tools offer many different ways to monitor and report on the online activities of minors; and

- **Policy Management Per User or Per Group:** Schools and libraries can customize their Internet policies based on users or groups, so policies can be set based on age or needs.

The Children's' Online Privacy Protection Act (COPPA) must not be violated by any requirements of the filtering solution to collect personal information about students. Refer to http://www.ftc.gov/ogc/coppai.htm for information about COPPA.

All Websense data is logged and retained in a Microsoft SQL Database. Websense can leverage directory information from your LDAP infrastructure to map policies to directory objects instead of IP addresses. When users are identified and receive the appropriate policy based on the directory information, all traffic logs are sent to a SQL Server retaining this information and running in your environment. Websense does not retain any sensitive/non-directory information in our solution. We are also ISO27001-certified.

Section I - Current Environment

The Internet filtering shall be done at the two POPs where the K-12 network is routed to the ISP.

Yes. You can leverage multiple policy servers at each point of presence. All policy servers can be centrally managed from one location/interface.

If the server specifications and/or the number of servers listed above are not capable of fully supporting the vendor's filtering solution, the vendor must include all appropriate servers or appliances and associated costs in the response to this RFQ.

Websense Web Security can be easily scaled to handle your internet traffic. While peak bandwidth utilization of up to 10Gbps is being asked for, we would like to know your current realistic utilization of this internet pipe per POP. Three reference deployment options are provided in the response to "Scaling," below.

The Internet filtering must occur at the points in the network after which the K-12 core routers consolidate Internet traffic but before the firewall dynamically changes the private IP addresses to public IP addresses as shown in the diagram on attachment A.

Websense Web Security can be deployed using multiple options. The most common deployment method consists of leveraging our Network Agent (Standalone) which is response for sniffing a SPAN port using your core switches or network taps. You may also choose to integrate us using your Cisco PIX.

List of Common Deployment Options:

- Standalone/SPAN: Leverages a SPAN port to filter all traffic
- Integrated: Integrates using the following vendors/methods:

Product	Versions
Microsoft Forefront TMG	2008 or later
Cisco PIX Firewall	v5.3 or later
Cisco ASA	PIX v7.0 or later
Cisco Content Engine	ACNS v5.5 or 5.6
Cisco Router	IOS v12.3 or later
Check Point	Firewall-1 NGX, NGX 65, UTM-1 (VPN-1) Edge
Citrix XenApp	5.0 or 6.0

The filtering servers and reporting servers must operate within the scope of the K-12 private network so that filtering control and reporting will reflect the private IP addresses of the client computers.

Yes. The filtering servers and reporting servers operate within the scope of your private network to reflect the IP address/directory information of your client computers.

Remote Filtering: In the event that portable computers are connected to residential, public, or other networks, an option must be available to provide continued filtering of Internet web sites. No caching appliances are currently in use; however the Internet filtering solution must support the option for the WVDE to install caching appliances.

To centrally manage off-site district assets such as Windows PCs and laptops, and Mac desktops and laptops, the following option is available:

Remote Filtering Server (requires additional package purchase): Remote Filtering Server provides Web filtering for machines that are located outside the network firewall (e.g., laptops). A remote computer must be running Remote Filtering Client to be filtered by the Remote Filtering Server. Remote Filtering Server acts as a proxy that accepts requests from Remote Filtering Client and submits them for filtering. It communicates with Filtering Service to provide Internet access management of remote machines. These remote devices are still centrally managed from both a policy definition and reporting perspective and do not require any additional interfaces or policies to be managed.

Scaling: The quoted solution must be designed to accommodate peak usage at each of the two POP sites. Peak usage is defined as 100,000 computers, 140,000 users, and 10Gbps of bandwidth to the Internet at each POP site.

Websense Web Security deployments consist of the following components:

1. **TRITON Manager:** Centrally manages your WWS solution from both a policy definition and reporting perspective. This is a web-based interface;
2. **Filtering Server:** Responsible for filtering your client computers and enforcing policies;
3. **Log Server:** Each filtering server sends all processed traffic to a log server in preparation for database logging; and
4. **SQL Server:** Responsible for retaining all traffic logs in a Microsoft SQL Database.

To provide the most customized response, Websense is providing the following deployment options based on your realistic internet pipe utilization. For example, if only 2Gbps out of your 10Gbps connectivity is being utilized, the numbers of servers needed today would be much different than 10Gbps of realistic utilization. Websense would like to provide you with the following deployments ranging from 2Gbps of realistic internet traffic up to 10Gbps. Each option highlights the number of servers needed associated with each of the components above.

2Gbps Internet Connectivity

Component	# of Servers Needed	Requirements/Specifications
TRITON Manager	1	Hardware: • 4 CPU Cores (2.5GHz + each) • 6GB RAM • 120GB of Disk Space Software: • Windows Server 2008 R2 x64
Filtering Server	6	Hardware: • 2 x Quad Core Xeon Processors (2GHz+) • 24GB RAM • 2 x 300GB HDD (SAS Preferred) Software: • Windows Server 2008 R2 x64
Log Server	1 for every 10,000 users when full URL logging is enabled	Hardware: • 4 CPU Cores (2.5GHz + each) • 6GB RAM • 250GB HDD Space Minimum (SAS + RAID) for best IOPS Performance Software: • Windows Server 2008 R2 x64
SQL Server	1	Hardware: • 1 x Quad Core Xeon Processors (2GHz+) • 16GB RAM • 1TB per your requirements (SAS + RAID) preferred for best IOPS performance Software: • Windows Server 2008 R2 x64 • Microsoft SQL Server 2008 R2 x64

6Gbps Internet Connectivity

Component	# of Servers Needed	Requirements/Specifications
TRITON Manager	1	Hardware: • 4 CPU Cores (2.5GHz + each) • 12GB RAM • 300GB of Disk Space Software: • Windows Server 2008 R2 x64
Filtering Server	18	Hardware: • 2 x Quad Core Xeon Processors (2GHz+) • 24GB RAM • 2 x 300GB HDD (SAS Preferred)

6Gbps Internet Connectivity		
Component	# of Servers Needed	Requirements/Specifications
		Software: • Windows Server 2008 R2 x64
Log Server	1 for every 10,000 users when full URL logging is enabled	Hardware: • 4 CPU Cores (2.5GHz + each) • 6GB RAM • 250GB HDD Space Minimum (SAS + RAID) for best IOPS Performance Software: • Windows Server 2008 R2 x64
SQL Server	1	Hardware: • 2 x Quad Core Xeon Processors (2GHz+) • 24GB RAM • 1TB per your requirements (SAS + RAID) preferred for best IOPS performance Software: • Windows Server 2008 R2 x64 • Microsoft SQL Server 2008 R2 x64

10Gbps Internet Connectivity		
Component	# of Servers Needed	Requirements/Specifications
TRITON Manager	1	Hardware: • 4 CPU Cores (2.5GHz + each) • 24GB RAM • 500GB of Disk Space Software: • Windows Server 2008 R2 x64
Filtering Server	30	Hardware: • 2 x Quad Core Xeon Processors (2GHz+) • 24GB RAM • 2 x 300GB HDD (SAS Preferred) Software: • Windows Server 2008 R2 x64
Log Server	1 for every 10,000 users when full URL logging is enabled	Hardware: • 4 CPU Cores (2.5GHz + each) • 6GB RAM • 250GB HDD Space Minimum (SAS + RAID) for best IOPS Performance Software: • Windows Server 2008 R2 x64
SQL Server	1	Hardware: • 2 x Quad Core Xeon Processors (2GHz+) • 32GB RAM Minimum (64GB Preferred) • 1TB per your requirements (SAS + RAID) preferred for best IOPS performance Software: • Windows Server 2008 R2 x64 • Microsoft SQL Server 2008 R2 x64

Section II - Technical Requirements

The vendor bid must provide an Internet filtering solution capable of filtering 200,000 total computers in a network consisting of two POPs with 280,000 users. The solution must be configured to support 100,000 client computers and 140,000 users using 10 gigabits/sec of bandwidth at each POP.

Please see the response to "Scaling," above.

The vendor must provide evidence of at least one current, successful installation of the Internet filtering solution in a network configuration servicing 100,000 computers and 140,000 users with 10 gigabits/second of Internet bandwidth. This evidence must include details regarding the size and scope of the successful project(s) as well as contact name(s) and phone number(s) for customer(s) where the successful Internet filtering solution was implemented. The vendor must submit a memo from the successful customer (on customer's letterhead, dated and signed) describing the size and scope of the successful project, as well as any issues (if any) and how they were resolved.

Websense, Inc. (NASDAQ: WBSN), delivers the best content security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market, and small organizations around the world.

Customer size ranges from several hundred employees to tens of thousands of employees. Our customer base ranges from finance, banks, credit unions, healthcare, technology, communication, government, education, to other various smaller businesses and organizations. Many customer video case studies have been done. You can find them by the various products at: http://www.websense.com/content/CaseStudies.aspx.

Examples of Websense WWS customers include:

- Brisbane Catholic Education;
- InfoNet Services Corporation; and
- Commonwealth of Pennsylvania.

Websense does not issue contact or project details for customers without seeking the appropriate agreements from them. However, upon request we will be happy to arrange reference calls with appropriate customers at a later stage in the sales cycle.

The filtering solution must be a POP based installation capable of providing a level of service appropriate for an Internet Service Provider (ISP); a filtering solution which involves the installation of filtering software or hardware within school districts or individual schools is not acceptable.

All Websense Web Security (WWS) components can be deployed in your data centers. WWS can easily monitor your network points of aggregation.

The vendor must provide Internet filtering and reporting application software and all necessary supporting software including, but not limited to, operating system and database software.

In addition to the WWS software, the following applications will be needed that are not included with the proposed solution:

- Microsoft Windows Server Licenses; and
- Microsoft SQL Server Licenses.

For further information on the utilization of the additional applications stated above, please see the response to "Scaling," above.

The Internet filtering solution must meet the requirements of this RFQ using servers/appliances provided by the vendor or when installed on the WVDE owned equipment identified in Section I - Current Environment.

Please see the response to "Scaling," above.

The filtering solution must support gigabit speed, copper based, Ethernet network interfaces.

Yes. WWS supports gigabit connectivity per your requirements.

The filtering solution must not exceed a total of 12 servers or appliances at each POP.

Please see the response to "Scaling," above.

The total of all hardware components of the filtering solution for each POP must be rack mountable and not occupy more than 24 units of rack space (about 48") at each POP site. The equipment must operate on 110-120 Volts AC power.

Please see the response to "Scaling," above.

In the event the winning bid does not meet the requirements of this RFQ when installed on vendor provided server/appliances or on the existing equipment identified in Section I-Current Environment, the vendor must provide additional servers and any other associated installation, shipping, labor and configuration expenses at no cost to the WVDE or the contract will be immediately terminated.

We understand hardware is required as part of the solution, however based on the requirements set forth within the RFP, we believe further discovery is required in able to provide the optimal solution. At this point we are submitting a software and professional services proposal only, and if given the opportunity for further detailed discussions, we will be able to provide the complete solution to meet your requirements.

There must be no requirement for any configuration changes of any networking equipment or computers that are connected to the private WV K -12 network at the school districts or individual schools.

Websense Web Security offers multiple deployment methods (highlighted in detail above). Typically, depending on the desired deployment method, we can either a) leverage your Cisco PIX Firewall; or b) leverage SPAN ports in your network provided by you.

The filtering solution must provide client software which can be installed on mobile computers that will enforce the same filtering parameters whether a mobile computer is connected to the WV K-12 network or connected by wired or wireless networking to the Internet via any other Internet service provider. The client software must not be a VPN (virtual private networking) or similar type of client and must not rely on a web browser setting such as proxy server configuration.

Our remote filtering client software can enforce the same filtering parameters on outside/remote networks. A remote filtering server will need to be brought up in the DMZ of your network. For detailed information on Remote Filtering Server, please review the "Remote Filtering" section above. The filtering client software operates at the kernel level of the OS to prevent bypassing.

The filtering solution must have the capability to filter based on the IP address of the client computer and not require user authentication.

Yes. WWS allows you to define and enforce policies based on the IP address of the client computer.

The filtering solution must have the capability to be integrated with unified authentication systems such as LDAP and Active Directory service.

Yes. WWS can be integrated with directory services such as Microsoft Active Directory for authentication.

The Internet filtering solution must be engineered and operate with redundancy such that the failure of one server or appliance at a POP will not reduce the capability to provide filtering for 100,000 computers and 140,000 users at 10 gigabits/sec of throughput.

WWS can be deployed to handle High Availability scenarios; however, HA scenarios will need to be discussed with you in detail so that SHI can best tailor a deployment plan for you.

2.1.2 Internet Filtering

The filtering solution must provide a web based interface for all management and configuration tasks which can be performed by WVDE.

Yes. Our TRITON Unified Security Center is a web-based interface that allows you to manage and create policies as well as run reports from a centralized console.

The filtering solution must have the capability to be configured to block Internet access in the event of the failure of the filtering solution at a POP so that unfiltered Internet access is prevented.

Yes. You may configure Websense Web Security to fail-closed.

The Internet filtering solution provided as a result of this RFQ must be verified by the vendor to meet the requirements of the Children's Internet Protection Act (CIPA) (refer to http://www.fcc.gov/guides/childrens-internet-protection-act) and the West Virginia Board of Education Policy 2460 which is available online at http://wvde.state.wv.us/policies/policy.php?p=2460&alt=1.

Websense Web Security products can help make the Web a safer place for your students. We can:

- Filter inappropriate content, malicious code, and other threats;
- Control access to protocols such as IM, P2P, and streaming media;
- Provide controlled social media access; and
- Prioritize network access according to users, time of day, and other parameters.

Specifically, CIPA states that technology protection measures (filtering solutions) must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors. The filtering solution must block access to this CIPA specified content.

Yes. We are able to accomplish this with the use of our safe-search filtering option.

CIPA also states that schools receiving E-Rate must monitor the online activities of minors. Therefore, the Internet filtering solution must include the ability to configure logging of all allowed and blocked Internet requests.

Yes. Websense Web Security allows you to log either the URL hostname, the default option, or you may enable full URL logging for all URLs both blocked and permitted.

The filtering solution must be verified by the vendor to comply with the Children's Online Privacy Protection Act (COPPA) (refer to http://www.ftc.gov/ogc/coppa1.htm). The filtering process must not require the collection of any personal information from any users under the age of 13.

All Websense data is logged and retained in a Microsoft SQL Database. Websense can leverage directory information from your LDAP infrastructure to map policies to directory objects instead of IP addresses. When users are identified and receive the appropriate policy based on the directory information, all traffic logs are sent to a SQL Server retaining this information and running in your environment. Websense does not retain any sensitive/non-directory information in our solution. We are also ISO27001-certified.

The filtering solution must provide the capability for the WVDE to selectively enable filtering of content based on categories of web sites or individual web sites using the http and https protocols.

Yes. Websense Web Security's master URL database comes with 90+ predefined categories that you can permit, block, confirm, or configure to use quota time for categories and individual sites using HTTP/S protocols.

The vendor must include all categories that the vendor offers on the product. The vendor must not offer a reduced number of categories in an attempt to reduce costs by providing only the categories that are identified in this RFQ.

Websense Web Security comes with an extensive list of categories. All WWS categories are provided out-of-the-box.

The vendor must provide, but is not limited to, the pre-populated categories of the following classifications or equivalent classifications of content on web sites:

- Pornography
- Obscenity
- Dating (including sites for the purpose of establishing personal relationships)
- Gambling
- Criminal Activities (sites that condone or provide instructions for criminal activity)
- Illegal Drugs (sites that condone or provide instructions for illegal drug use, manufacturing and distribution)
- Anonymous Proxies (anonymizers to bypass filtering or hide the true source of Internet activity)
- Computer crimes, cracking and hacking (sites that condone or provide instructions for these activities)
- Malicious code (sites that contain, distribute, or execute malicious code such as mal ware, viruses, root kits, bots, etc or retrieve information from computers that are infected with malicious code)
- Instant messaging sites
- Peer to Peer (P2P sites)
- Phishing (fraudulent sites that imitate authentic sites, often to lure people into submitting personal or financial information.)
- Hate, racism, discrimination (sites that condone or encourage violence against or suppression of any minorities or grouping based on race, religion, sexual orientation, ethnicity or any other social grouping characteristic)

Yes. Websense Web Security offers these categories or similar categories to prevent your students from browsing malicious or inappropriate content.

The filtering solution **must** have the capability to allow or deny access to any individual web site, URL, or IP address whether or not it is included in any vendor provided category.

Yes. Websense Web Security allows you to categorize or re-categorize specific URLs or IP addresses to better fit your district needs.

The filtering solution **must** have the capability to permit the WVDE to create unlimited additional custom categories.

Websense Web Security allows up to 100 custom categories to be created.

The filtering solution **must** have the capability to permit the use of "regular expressions" (includes wild-card characters and other variables to specify complex text strings) when creating custom allow or deny lists of URL web addresses or search terms.

Yes. Websense Web Security does allow for the use of regular expressions for categorizing and re-categorizing both allowed and denied URLs.

The filtering solution **must** have the capability to block traffic related to peer-to-peer file sharing protocols.

Yes. Websense Web Security is able to block peer-to-peer file-sharing protocols that attempt to initiate a TCP connection upon application launch or sign-in.

The filtering solution must have the capability to enforce the "safe searching" mode of Google, Bing and Yahoo search engines, regardless of the settings chosen by an end user while accessing those search engines.

Yes. Websense Web Security offers safe-search image filtering from the following search engines:

- Ask;
- Bing;
- DuckDuckGo;
- Google;
- Lycos;
- Yahoo!; and
- Yandex.

The filtering solution must provide capabilities to create manageable client groups based on IP address ranges and assign names to those groups.

Websense Web Security allows you to apply policies in a variety of ways, such as by Active Directory (AD) User, Group, OU, workstation IP, network range, or the default policy.

The capability must exist to delegate management of groups by creating additional administrators with restricted rights who can be assigned to manage filtering parameters for specific groups.

Our Web Security product has the ability to provide role-based access for different administrators using our Delegated Administration feature. This gives you the granularity to identify not only who has access to the module, but also what they are able to see or modify (e.g., Policies, Reporting, or both).

The filtering solution must provide for customizable, granular permissions so that additional administrator/user accounts can be tailored on a user by user basis to match the rights of a user to the tasks that a user needs to perform.

Websense Web Security also allows you to identify managed client(s) to those delegated administration roles. You may designate specific administrators/managers to manage/report off a particular user/group, etc. if desired.

The filtering solution must have the capability to selectively display WVDE customized "site blocked" pages based on the client group and/or the categorization of the blocked web site.

Websense provides the ability to fully customize your block page using a HTML editor. A list of tokens is available on our support site.

The filtering solution must have the capability to selectively display WVDE customized "informational" pages based on the client group and/or the categorization of web sites to which access is allowed.

WWS does not have the ability to display "informational" pages on allowed sites. The closest option would leverage our "Continue" disposition option on specific categories. You will be able to modify the informational message displayed to the end-user. This would allow your end-users to review the informational message prior to viewing the requested site by clicking on the "Continue" button.

The filtering solution must have the capability to be configured to only perform filtering of outgoing requests and to perform no filtering of incoming traffic.

Websense Web Security will filter Web traffic (originating from inside your network) making a request to a website outside of your network.

The product offered by the vendor must perform Internet filtering primarily by comparing outgoing requests to a database of categorized URLs and IP addresses to determine whether an attempt to access a site on the Internet is to be blocked or permitted.

The Websense Master Database contains the industry's most accurate, current and comprehensive classification of URLs. We use proprietary classification software and human inspection techniques to categorize and maintain definitions of more than 90+ categories in more than 50 languages.

Any other Internet filtering methods of the filtering solution, such as "on the fly" evaluation of incoming content, must be able to be selectively disabled at the option of the WVDE.

Websense Web Security does not perform real-time scanning techniques.

The filtering solution must provide a web based display of status and performance graphs for all components of the filtering solution.

Upon login, our Web Security product gives you access to multiple dashboards that allow you to review your web security and system health posture. Websense Web Security also provides dashboards that display top risks, top usage reports (e.g., user, category, etc.) as well as system health alerts to identify current communication of Websense components. Each of these dashboards can be customized to suit your needs. Additional dashboards can be added from a list of available options.

The filtering solution must have the capability for the WVDE to set customized filtering policies based on the time of day and the day of the week for individual IP addresses and/or groups of client IP addresses.

Yes. Websense Web Security allows granular control over policy definitions such as identifying the time of day, day(s) of week, etc. for a specific IP, user, or group.

The Internet filtering solution must not masquerade, spoof or change the source IP address of the computers on the K-12 network. The source IP address of the client computer must be passed to the PIX firewall.

Our Web Security product is not a "man-in-the-middle" solution; therefore, IP spoofing of client IP addresses does not occur.

The Internet filtering and reporting servers must operate on and report on the 10.0.0.0 private network IP addresses of the WVDE K-12 network.

Yes. We can operate and report on any Class A, B, or C subnets. Therefore, the 10.0.0.0 private network IP addresses will not be a problem.

The filtering solution must have a synchronization capability. Synchronization means that when the WVDE makes a filtering configuration change using the web management tool, that change will be distributed to all of the filtering servers at both POPs. That change distribution must take effect automatically within 5 minutes after the act of saving the configuration change, or be accomplished manually with no more than 5 mouse clicks after the configuration change is saved.

Yes. Each Policy Server will point to our Policy Broker which shares a centralized Policy Database. Therefore, when changes are made on one Policy Server, they will be distributed to the other Policy Servers as well.

2.1.3 Internet Use Reporting

The filtering solution must provide a web-based reporting application and a minimum of one terabyte of log file storage at each POP.

Our Reporting Tools are web-based and will be able to query your SQL database. However, a terabyte of data is significant amount of data to run a report against. Furthermore, the log file storage will be dependent on your SQL Server's hardware specifications.

The filtering solution must provide a method for the WVDE to download log files in a generic text format for analysis and archival storage.

Audit logs and our reporting logs may be exported to an XLS file.

Complete details of web browsing activity must be stored in log files and must include, at a minimum, the complete URL, date and time and IP address of the client computer.

Our Reporting Tools, by default, include the URL hostname only. However, as long as you have enabled full URL logging, you may modify your report(s) to include the full URL as well as other report criteria.

All end user functions of the reporting application must be accessible via a web interface.

Yes. Our reporting tools are accessible via TRITON Unified Security Center, a web-based interface.

The reporting solution must provide the capability to create reports based on specific IP address, web site address, date and time of day.

Yes. Our reporting tools will allow you to run reports based on specific IP address, Web site URL, and others.

The reporting capabilities must include the ability to schedule aggregate reports of web site accesses by categories, ranges of IP addresses and time periods.

Our reporting tools allow you to run reports and save them as favorites. These reports may then be scheduled to be run once, daily, weekly, or monthly. You may also schedule these to run and be emailed to administrators/managers of your choosing.

The reporting capabilities must include the ability to create "on demand" custom reports on selected client IP addresses, specific URLs and time periods.

Yes. Our Web Security product offers the ability to create custom reports.

2.1.4 Invoicing

The costs for software and the annual licensing for Internet filtering shall be invoiced upon delivery and acceptance by the WVDE. The technical support costs are payable in arrears according to the State of West Virginia terms of payment and shall be invoiced not more than one time per month."

The Websense standard technical support is included with the Websense licensing. Invoices for implementation services will be sent after completion of services, not more than one time per month.

2.1.5 Vendor Requirements

The vendor is solely responsible for all work performed under the contract and for all services offered and products to be delivered under the terms of this contract.

If the successful vendor is not the direct source, the vendor must provide documentation of being an authorized reseller to provide the equipment, filtering updates, maintenance and technical support. This documentation must be provided upon request from Agency.

This documentation will be provided upon request from Agency.

2.1.6 Service Requirements

The vendor must provide modification or replacement of software that fails to perform according to the specifications. The vendor also must provide any software upgrades, at no cost to the WVDE, that are necessary during the term of the contract in order to continue to meet the Internet filtering capabilities specified. This requirement includes replacement, at no cost to the WVDE, which may be necessary due to possible end-of-life designation by the manufacturer.

Websense provides a major release every 6 months. Patches and hot-fixes are released as needed. Users are notified by email alert for software updates. These updates are all included as part of the maintenance plan. Older versions will be supported 2 years after their end-of-life, announced by Websense.

The appliance OS includes a patching mechanism for itself, as well as application modules.

The filtering solution installation, configuration and testing at both the Charleston and Morgantown POP sites must be completed by the vendor within 30 days after the award of the contract. The vendor is responsible for any transportation, and lodging costs of the installer, as well as for any freight or shipping charges for equipment.

Evolve Technology Group understands and will comply in order to meet your implementation timelines.

The Internet filtering solution must support the bandwidth requirements of 10 gigabits/sec and 100,000 client computers/40,000 users at each one of the two POPs as identified in the specifications in Section II-Technical Requirements.

Please see the response to "Scaling," above.

Toll-free telephone and e-mail technical support must be available 7:00 AM to 5:00 PM Monday through Friday, Eastern Time (GMT -0500) for designated WVDE networking staff. Any costs associated with this requirement are to be included in the line item for technical support on the cost page.

Websense Technical Support combines people, process and technology in support of our Subscribers' use of Websense Products. Subscribers are enrolled in one of three Websense Technical Support programs: 1) Standard Support; 2) Premium Support; or 3) Mission Critical Support. Standard Support is included with a Subscription upon payment of the associated Subscription Fees. Premium Support and Mission Critical Support are additional charge support options, and are only provided after Subscriber has paid the associated fees for participation in one of these two support options.

1. Websense Standard Support: Websense Standard Support is included with the Subscription. Through the combination of available resources, Subscriber can submit new cases and manage case status, access the latest security features and download software, upgrades, updates and patches, as well as review Websense Product documentation. With Standard Support, Subscribers receive:

    - Access to the Websense KnowledgeBase;
    - Access to Websense Customer Forum;
    - Tech Alerts Subscription;
    - Web support via the eSupport portal;
    - Access to MyWebsense, a secure portal to submit and track cases, download software updates and patches;
    - Five (5) incidents per Subscription year for telephone and online access to technical support engineers during Websense normal business hours for the region where Subscriber is located;
    - 24/7/365 access to the online Websense Web portal located at: http://support.websense.com; and
    - Four free web-based training sessions per year.

2. Websense Premium Support: Websense Premium Support includes all the benefits of Standard Support on a 24/7 basis, including weekends and holidays. In addition to those benefits included in Standard Support, Premium Support includes:

    - Access to a toll-free number for support requests;
    - "Follow-The-Sun" support for Severity Level 1 issues;
    - No limit on the number of incidents per Subscription year for telephone and online access to technical support engineers during Websense business hours;
    - Priority access to technical support engineers;
    - Priority email support;

- Submit 5 URLs at a time for Site Categorization;
- Site Categorization Priority; and
- Severity two, three, and four issues will be worked during regular business hours only.

3. Websense Mission Critical Support: Websense Mission Critical Support combines all the benefits of Premium Support with a technical account manager (TAM) who is assigned to the account, and who proactively works with the Subscriber to support performance, reliability and availability of the Websense Products. Upon gaining an understanding of Subscriber's environment, the TAM will work with Subscriber to:

   - Provide strategic support planning around Subscriber's use of the Websense Products; and
   - Perform architecture reviews, migration planning assistance, training recommendations and periodic account reviews.

With Mission Critical Support, Subscriber receives access to:

- A designated senior technical support engineer;
- A single point of contact for support inquiries;
- Collaborative strategic support planning; and
- Expedited case handling and escalation path.

These benefits are described in more detail on the Websense Support Portal at: http://www.websense.com/content/TechnicalSupportPrograms.aspx.

The vendor must provide a function that permits any user of the WV K-12 network to submit a web site to be reviewed and appropriately categorized by the vendor. This function allows the vendor to receive feedback with the intent of improving delivery of services or product functionality.

Miscategorized websites can be submitted for review using the Websense site look-up tool online or by submitting the URL to suggest@websense.com.

2.1.7 Vendor Response

The vendor shall complete the Cost Worksheet.

Evolve Technology Group agrees and has complied.

The vendor must provide evidence of at least one current, successful installation of the Internet filtering solution in a network configuration servicing 100,000 or more computers/40,000 users with 10 gigabits/second or more of Internet bandwidth. The following table shall be used in the vendors response.

Project Name	Contact name and phone number	# of computers filtered	# of users supported	Internet bandwidth
Sutter Health	Contact will be provided upon request.	100,000	40,000	620 MB

State of CA	Contact will be provided upon request.	100,000+	150,000+	1-10gb, depending on location

If the vendor fails to identify any costs that are required to meet the terms, requirements and conditions of this Quotation, it **shall** be the responsibility of the successful vendor to pay those costs and such costs will not be passed on to the WVDE or the State of West Virginia.

Evolve Technology Group understands that hardware is required as part of this solution, however based on the requirements set forth within this RFP we believe that further discovery is required in order to provide the optimal solution. At this point, we are submitting a software and professional services proposal only. If given the opportunity to engage in further discussion.

Pricing **must** be stated on the basis of one-year contracts.

Evolve Technology Group agrees and has complied.

Filtering licensing prices **must** be quoted based on the number of users filtered annually so that the WVDE can determine the basis of the pricing submitted in the quote.

Evolve Technology Group agrees and has complied.

Software updates/upgrades and technical support **must** be priced on an annual basis and this item is reflected as such on the cost page.

Updates and upgrades are all included as part of the maintenance plan. Costs for Premium and Mission Critical Support are provided on the cost page.

The vendor is responsible for any costs due to product end of life that will require replacement or upgrading of the vendor provided software or hardware during the term of the contract.

Evolve Technology Group agrees and will comply. Websense provides free updates during the term of your subscription.

3. Miscellaneous

3.6 Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Anthony Lange
Telephone Number: 916-295-1595
Fax Number: 916-577-1076
Email Address: alange@go-evolve.com