Blue Coat ProxySG Project

Chris Candilora
Cortland Clater
Eric Garner
Justin Jones

Background, Motivation, Objective

There are two major focuses of the Blue Coat Proxy SG line. 1) Provide a secure web gateway for a network in a bidirectional forward proxy setup. 2) Improve network performance and optimization through bandwidth management and proxy caching.

Securing the Network

The Proxy SG device is placed inline with incoming connections and acts as a filter for all types of traffic monitoring and control. Malware is all over the Internet and a large portion of it resides on sites that appear to be legitimate. Web 2.0 applications have complicated and compounded the malware problem. With Web 2.0 users are able to receive content on the fly and this presents a major problem for the traditional signature-based methods to prevent malware from spreading. Additionally, with the emergence of social media websites personal information is readily available for attackers.

Email continues to be a target for new and unsuspecting users. Attackers are continually refining their techniques and improving their email tactics. Through the use of cloning emails from legitimate businesses – attackers are able to gain all sorts of personal information through cross-site scripting and malicious code/links. Enterprises with large email systems are especially vulnerable to internal attacks and the loss of trade secrets or corporate information.

All of the threats present a great opportunity and challenge for the security products sector. With large organizations the vast number of attack methods make it difficult to incorporate an all-in-one solution. Additionally, organizations are looking for custom solutions that implement with systems they already have in place. This requires vendors to be flexible and have the ability to turn on/off features and customize deployments.

Another issue facing corporate environments is the proliferation of satellite offices, telecommuters, and mobile phones. The changing landscape provides attackers many additional opportunities to compromise network security. The remote user and device poses serious security risks and adds a new layer of difficulty to protect organizations or personal information.

Blue Coat is one of the market leaders in providing a solution with an array of protection options. This is one of the key differentiators between the Blue Coat systems and some of the competitors. The value added options of having a multi function appliance is also one of the product issues Blue Coat faces. One of the biggest set backs with their equipment their inability to update their massive array of features frequently. Companies in more niche markets have been quicker to adapt to the latest threats and this is a problem for Blue Coat.

As the threat environment continues to be more complex and sophisticated – the emerging market leaders will adopt business models that provide agility and flexibility to manage new threats. The focus is moving to real time threat detection. It will continue to be important to maintain databases of phishing sites and signature threats, but (more importantly) security software and appliances will need to implement real time threat management solutions. This sector is still in its infancy and provides an opportunity for new vendors to acquire market share. Blue Coat has been slow to update their product line to be more robust in real time threat management.

Network Performance and Optimization

As network traffic continues to increase exponentially the bandwidth available is always lagging behind. It is becoming more and more vital for organizations to manage their traffic and provide faster applications for clients and internal users. With the increasing use of bandwidth intensive applications and protocols organizations need to be able to prioritize the network traffic. This is most important in WAN setups where bandwidth is expensive and for some organizations is a large operating expenditure.

Organizations have many types of network traffic and it is crucial for organizations to manage the traffic and optimize their systems for the vital network traffic. Network performance can hinge on many factors (e.g., lack of bandwidth, excessive latency, poor traffic prioritization, unwanted traffic or low priority traffic). The emergence of cloud computing and more centralized infrastructures will continue to increase the demand on networks.

The biggest issue organizations are facing on their internal networks is swamping their WAN connections with non-mission critical traffic. This is an area where the Blue Coat system is extremely advanced and provides organizations with significant value in managing traffic and protocols. The Proxy SG series offers a massive array of options for bandwidth management. This is a two edged sword because traffic management requires significant CPU power it may not be a cost effective solution for many organizations. Faster and more efficient networks usage is a primary goal for organizations, but it must be cost effective. In some situations it may be more cost effective to simply add more bandwidth.

Another primary objective is to provide fast application response for their clients and users over the Internet. This is where the reverse proxy/internet acceleration abilities of the Proxy SG appliance make it one of the premiere offerings from Blue Coat. Reverse proxy setups allow an organization to scale horizontally extremely efficiently as demand for an application or service increases. It also offers improved security and flexibility for the internal original content servers. This significantly mitigates the risk when the network is compromised and adds another layer of security. For organizations that practice defense-in-depth this increases the number of hops for an attacker to reach the original application/content servers. In a reverse proxy setup the Proxy SG acts as if it is the original content server. In the commercial market, Blue Coat is a leader in reverse proxy setups, but there are viable open source solutions quickly closing the technology gap.

Motivation and Objective

Our motivation is to gain valuable knowledge IT architecture and infrastructure knowledge that will ultimately increase our value to organizations. Blue Coat is the market leader in enterprise network performance and security solutions. We feel there is great value in understanding their products and service offerings. The foundational knowledge required to setup the Blue Coat Proxy SG appliance required research into niche areas of the IT world that were not covered in regular courses.

Our objectives are clear: 1) Gain an in-depth understanding of enterprise security appliances and network optimization. 2) Understand the issues, requirements, and implementations of large organization's infrastructure bandwidth requirements, management, and acceleration.

Process and Approach

As we as a group looked to understand how the Bluecoat proxy SG functioned, we used several process and approach methods to help us get a better grasp on what, up to that point, was relatively unknown hardware. The process we used was, in large part, trial and error. Although many of us had some experience working with routers and other networking devices, Bluecoat's proprietary devices and their respective software interfaces were a new challenge. We found that many of the lessons learned were done by simply experimenting with certain Proxy SG utilities and observing the resulting outcome. Although not always the quickest and most efficient approach to learning, we found that we were able to gain a great deal of knowledge in a relatively short amount of time. In addition, we were able to gain valuable experience from others who had implemented similar hardware in real world environments.

When we first began working on this project, we decided as a team that we should try to learn as much as we could about how the Proxy SG device worked. We did this not only to be more knowledgeable for the ensuing masters project, but also to give us a broader palette of IT skills to help further our professional careers down the road. We approached this goal by making the decision to split up the main areas of the Proxy SG's functionality. We concluded that if each member of the group took a specific area, they could become experts in that particular area and then teach those concepts to the rest of the group. As each member learned something new about the Proxy SG, the team as a whole benefitted from that newfound knowledge. We feel this approach was successful because it allowed us to break an otherwise overwhelming amount of work into smaller and more manageable pieces. We relied heavily on one other and depended on our group members to bring valuable knowledge and a strong work ethic to the table. To better understand how Bluecoat's hardware worked, we were fortunate enough to procure the Proxy SG appliance from Dr. Randy Boyle. He allowed us to use this hardware device to understand how it functioned. In addition, we were able to secure two server devices to help us create a realistic test environment for our proxy device. This approach was extremely beneficial for our group because it allowed us to see a direct cause and effect of our actions in a contained environment without fear of repercussions. We regularly worked within this contained environment and implemented a variety of experimental changes and observed the direct outcome of those changes. We experienced our fair share of both failures and successes using this approach but we were able to gain valuable hands-on experience that would have been difficult to obtain otherwise. This makeshift test environment was where we picked up the majority of our Proxy SG skills and expertise.

In addition to first hand experience, our group benefited from learning from other businesses and institutions that had implemented Bluecoat hardware in their own production environments. Several members of our group had direct connections or were able to seek out IT professionals who were willing to share their knowledge and opinions on how best to utilize the Proxy SG device. This provided us with a great resource of information as we were able to get a third party perspective and were allowed to get a glimpse into how best to implement Bluecoat's hardware in a real world production environment. In addition, we were able to obtain training documentation from these third party contacts, which allowed us to better understand the Proxy SG workflows and processes. These documents would not have been available to us otherwise and added to our basic understanding of the how the hardware worked.

To help ensure that project deadlines were met, our group met regularly and maintained a schedule of when key milestones should be completed. Our group meetings served to not only brief one another on the new concepts we learned, but also as a way to reinforce team goals and expectations of one another. This was a successful method and ensured that all team members stayed on task were apprised of what they should be focusing on at that particular point in time. Our team was extremely productive during these group meetings and we were able to cover a great deal of material in a relatively short amount of time. We met in a variety of locations, both on and off campus and were able to contribute equally to the final project.

Results

The Proxy SG device contains a multitude of different options, features, and services. While we explored most of the device's functionality, our limited time and manpower forced us to narrow down our focus for the report and presentation. In the end, we wanted to focus on those areas of service that were the most used, useful, and powerful. After extensive research, and hands on use, we determined that web filtering, bandwidth management, proxy services, reverse proxy services, and the application delivery network were the features that we really wanted to spotlight for our report and presentation. While these are the areas that we have chosen to explain and demonstrate, it should be noted that we are also very knowledgeable about the other features that are made available on the ProxySG device. For example, other services like statistical analysis and hardware/software maintenance were used extensively. In addition to focusing on functionality, we also explored how these devices are used in real world settings. Specifically, we spoke with representatives from the University of Utah Hospital and the LDS Church to gather some results on how Blue Coat proxy devices have affected their respective organizations.

We set out to accomplish two things with this project. First, we wanted to understand and experience the full functionality of the proxy device. Since we were able to learn and effectively use most of the services offered by the Proxy SG, we believe this first goal was accomplished. Our second goal was to determine if a Blue Coat Proxy SG appliance is a viable product for the University of Utah. From understanding the functionality of the device and by speaking with two large and complex organizations, we were able to accomplish this second goal as well. The rest of this section explores both of these two goals in depth.

To begin, we will focus on our results in regard to the specific functionality of the Proxy SG device. We discovered that web filtering is by far the most useful and widely used service available. While many of the devices are useful in only very specific circumstances, web filtering is needed in virtually every organization, every second of the day. The main benefit of implementing a web filter is that it blocks traffic based on website categories. These categories have all been classified by Blue Coat and include categories like pornography, gambling, social networking, and hundreds of others. Blocking specific website content has many advantages. Most importantly, it limits users from accessing harmful sites that are likely to transmit different types of malware. Furthermore, it allows users to only access more productive websites and keep off of time wasting ones likes Facebook, ncaa.com, and many others. Finally, by blocking these types of websites, the organization is able to cut down on wasteful bandwidth usage which frees up more resources for the rest of the network. During our time with the Proxy SG device, we were able to set up the web filter, install the proxy client on the user's machine, and successfully block websites that we did not want the user to access.

Moving on, bandwidth management was the next service that we focused on. This service guarantees that certain classes receive a specific amount of the available bandwidth. Furthermore, certain classes can be given priority over others when only a limited amount of bandwidth is available. There are many situations where this service is needed. For example, a CEO might need a higher level of bandwidth speed than other workers in order to complete more important projects. This can easily be done by prioritizing his traffic based on his IP address. Another example would be to establish that resource hogging services, like video streaming, are given only a specific amount of the bandwidth available, if any. To accomplish tasks like these, we created management policies based on specific criteria, which included things like IP addresses, subnets, URLs, website categories, and time of day. During our tests, we were able to successfully implement bandwidth management policies based on virtually any network criteria that we desired.

Next, we explored the functionality of what Blue Coat calls proxy services. More specifically, the proxy services functionality allows users to block specific protocols, IP addresses, and ports. Many different protocols, like telnet and FTP, are vulnerable to attack by malicious users. Since most users do not need access to these protocols to complete their work, it is a standard safety procedure to block all of these protocols on all clients. The Proxy SG allows administrators to effortlessly disable any dangerous protocols to keep their network secure. Moreover, blocking specific IP addresses is often needed when certain external malicious users probe and attack the network. In this case, network administrators often want to "black hole" that user's IP address to keep them from accessing the network at all. Again, by using the Proxy SG device, network admins can create a new proxy service group, specify the IP address, and have it blocked within minutes. Along those lines, service groups can be created to block specific ports that are often accessed by hackers and not needed open by organizations. Moreover, the proxy services functionality allows you to create static bypass lists and restricted intercept lists that exempt users and target users respectively from the proxy service groups. During the course of our project, we were able to successfully block any protocol, port, and IP address that we desired. We were also able to successfully create static bypass lists and restricted intercept lists based on the IP address criteria that we specified.

The application delivery network (ADN) is the next service that we wanted to explain and demo. The ADN delivers network applications and resources quickly and efficiently across a WAN setup. It provides both compression and secure communications to accomplish this delivery process. By quickly delivering internal applications to satellite locations on the company's WAN, the ADN system is highly useful for increasing bandwidth savings and decreasing downtime. In order to properly utilize the application delivery network, both an ADN server and an ADN client need to be properly configured. Setting up an ADN server involves assigning the subnet it will preside over, approving any peers that will be connected to the server, and configuring the necessary protocols and ports. Setting up the ADN client involves installing the Blue Coat client application on any peer machines. Peers are then sent updates on a regular basis from the server. Once installed, the client enables "Total Savings" and "Savings Over Time" tabs on the client machine. These two statistics report the bandwidth savings that were gained as a result of having the ADN enabled. Our group was able to successfully setup the ADN server, with the required settings, and install the ADN client on a peer machine. At this point, we were then able to analyze the statistics to determine the kind of bandwidth savings we were successfully achieving.

Finally, the reverse proxy service is the last area that we wanted to document for this report and presentation. The reverse proxy is essentially a server accelerator because it reduces response time to clients. So, while a proxy device is typically used to optimize inbound content, the reverse proxy switches this role and optimizes outgoing content. Just as servers accessing the proxy believe they are really accessing the client, the reverse proxy tricks clients into thinking they are accessing the actual server when in fact they are only accessing the proxy appliance. This is extremely important for security reasons. With this setup, hackers only have access to the proxy appliance when they think they are really accessing the server. This severely limits the attacker's ability to harm the internal network. Along with security improvements, the reverse proxy provides many acceleration benefits. For example, through caching, it reduces response time to clients and reduces the load and bandwidth usage on the server. By successfully enabling this feature on our own proxy SG appliance, we were able to implement and utilize all of the benefits mentioned above.

Now that we have described some of the most important functionality of the device, we look at the results of how these Blue Coat proxy devices are utilized in real-world environments. More specifically, we analyzed how they are implemented at the University of Utah Hospital and at the LDS Church. The University hospital currently uses multiple Blue Coat appliances across their network. As far as services go, they mostly utilize the web filtering service and the reverse proxy caching. The administrators at the University Hospital believed that the web filtering did a great job of protecting their internal network and that the reverse proxy increased speed and responsiveness to their internal applications. However, the admins also encountered problems with the appliances. For example, the bandwidth management service was not enabled due to lack of machine resources. In short, the hardware specifications built into their Blue Coat devices couldn't handle the immense CPU power it takes to manage bandwidth for their numerous client and server machines. Also, they encountered integration difficulties when trying to implement these devices on their network. The second organization we spoke with, the LDS Church, also uses multiple Blue Coat appliances on their network. Unlike the University Hospital however, these appliances are used exclusively in reverse proxy configurations. The robust content on their mormon.org site is cached on the proxy appliance when it is accessed by outside clients. To successfully accomplish this, they created a hybrid solution with F5 load balancers and original content servers. The LDS Church believed that the Blue Coat appliances allowed for effective horizontal scaling and traffic management. Furthermore, the reverse proxy service was able to protect their network against attacks and provide fast and responsive access to web applications. However, they did experience some issues as well. Specifically, the cost of ownership and maintenance was very high and Blue Coat's customer support was not helpful in solving many of the problems that they encountered. In summary, both organizations found their Blue Coat appliances to be effective, but only for limited purposes. Services like web site filtering and the reverse proxy caching very advantageous, but the majority of other services on the Blue Coat appliances were not used. Ultimately, these organizations decided that what few things the proxy appliance does really well are often not worth the cost of owning an SG appliance as a whole. As a result, both organizations are currently looking for solutions elsewhere.

Finally, from our hands on experience and knowledge from the case studies, we can begin to answer the question of whether implementing Blue Coat appliances on the University network is a viable solution. In order to answer this question, we need to consider the product as a whole. In conclusion, we believe that the proxy appliance is an excellent enterprise solution for web filtering, proxy services, and if the hardware supports it, bandwidth management. Furthermore, it is very effective for application delivery acceleration using the ADN and server-side bandwidth optimization using the reverse proxy. However, we discovered that these are mostly the only services that we, and the two organizations we spoke with, found effective. This is contradictory to Blue Coat's strategy of marketing the Blue Coat SG as an all-in-one solution, which it often is not. More specifically, the organizations we spoke with typically only use the effective features, like web filtering and reverse proxy caching, and then disable the rest of the device's functionality. The reason for this is that the other features are difficult to configure, do not implement well with other devices, and have very little documentation. While it might seem like a suitable approach to just use the Proxy SG for the things it does effectively, you should remember that you are paying a very high price tag because Blue Coat is marketing it as an all-in-one device. As such, organizations may essentially be paying for features they are most likely not going to use. So, more specifically, if the University is willing to pay a steep price for services that work extremely well, like web filtering and reverse proxy services, then yes, a Blue Coat implementation would be very effective. However, the University will be paying a premium price for likely just these few services, while the other services will most likely not be used due to configuration and integration issues. If this is not a desirable situation, it is important to remember that other similar solutions do exist. The drawback to this approach is that these other solutions will not support services like web filtering and reverse proxy caching as well as Blue Coat appliances currently do. In summary, if the funding and technical expertise is available, the University should strongly consider using a Blue Coat Device for web filtering and reverse proxy services. If not, then other simpler and more user friendly solutions should be considered.

Lessons Learned

As we evaluate the project as a whole, throughout all of the project life cycles, we find that there are a few lessons learned and opportunities for improvement. Many are inconsequential as the direction of our project objective was forced to change due to limitations of network access as well as license caps due to budgetary constraints. The following outlines a few of the lessons learned.

Choose wisely the location of a device and be sure to immediately configure a second method of remote login when altering the configuration files. During the setup phase of the BlueCoat SG, there were a few occasions when specific configurations were made which "killed" our web access to the device. This resulted in a huge amount of wasted time in that we were not able to work on the device again until access was restored. However, the device was stored behind a locked door that no one in the group was able to access without the help of one of the professors. We found that the only way we could help the remedy our limited access to the device was to configure a secondary method for remote login through an SSH console. This proved to be very useful on a few occasions to help reverse some bad configurations that were not reversible through the universal web configuration.

Research out the connected network to make sure that the project objective is even doable. We realize that this restraint is mainly applicable to us in that we were trying to hook the BlueCoat SG to the university's network. However, we feel that this same situation may be applicable in situations where a contracted person configures a device to connect to someone else's network. It may not be possible to do due to the configurations of the system, security policies, etc. In our case, the university would not allow us to connect the BlueCoat to any network due to their limited control over the device and ignorance to its functionality. This is why extensive research and permissions for a project such as this is very necessary. We unfortunately did not realize that we would not be able to setup the device up on any functioning school network as a testing ground.

A proper project plan is necessary. From the beginning we had planned out what we were going to each do to setup the BlueCoat, however, we never really planned out implementation of the device. Setup proved to be fairly easy as we simply learned what each "useful" function of the device did and turned it on if it helped us accomplish what we were trying to do. However, when it came to implementation of the device for testing, we found that we were at a loss as to what to do. We had assumed that we were going to be able to connect the device to our local network and run it on actual student computers. However, this was not the case. Do to our lack of implementation planning we were forced to take an alternate route and build our project implementation phase around more of a consulting and research objective. We configured the device, tested it against a client computer, found the pros and cons of using this particular device and then gave our professional consult as to whether this device would be a viable solution to help the university meet its networking needs.

Future Directions

Due to our experience in working with the BlueCoat device, our outside research on the device, cost, usefulness of BlueCoat resources as well as a few other factors, we can not recommend the use of the BlueCoat SG on the university's network. However, if we were to recommend the use of the device, through our research we found that there are many different routes that can be taken for proper future use of a BlueCoat network setup.

Once the BlueCoat device, one which serves to load needs on the school, is installed on the network we could then decide whether to split the school into zones and apply peer devices to connect with the manager device or whether it would be better to only apply primary devices and backup devices on the main pipeline in and out of the school's network. As outlined in the presentation, both of these solutions are viable, however, due to the lack of cooperation from the school's network administrator for information as to how the school's network is setup, we can not make a proper consult as to how the BlueCoat should be installed.

After implementation, the administrators can then begin to fine tune the settings of the device to produce optimal results for the network. This would allow for increased productive use for the already existing network as well as protection from harmful malware from the outside as well as the inner network. In addition, the correct setup of the BlueCoat device would help cut back on bandwidth costs to the school. Therefore proper future tuning of the device's setting is absolutely necessary to unlock the full benefits of the device's potential.

Once the network is fully setup and running the only thing that would need to be routinely done is that of regular maintenance, updates and upgrades. These updates should be applied once the research has been done to guarantee continued support and functionality of proper configurations. In all, continued active support of the device is absolutely necessary to provide optimal efficiency of the network as a whole.

Works Cited

Orans, Lawrence, and Peter Firstbrook. *Magic Quadrant for Secure Web Gateway*. Issue brief no. V2RA1 05272012. Gartner RAS Core Research Note, 25 May 2011. Web. 11 July 2011. <www.bluecoat.com>.