Masters Project
Proxy SG
Group Members

Chris Candilora
Cortland Clater
Eric Garner
Justin Jones
Blue Coat Products
Blue Coat Proxy SG appliances offer a comprehensive foundation for the Blue Coat Secure Web Gateway solution.

They also provide advanced WAN Optimization feature sets.
Specifications

- $70,000 to $150,000+
- Up to 15x1TB SAS
- Up to 64 GB
- WAN & LAN
- Unlimited employees
Blue Coat Proxy SG appliances are available in a variety of form factors and performance levels appropriate for IT infrastructure environments ranging from small to medium enterprise branches to regional and core data centers.

- Protect users and networks from web threats, phishing and other attacks
- Accelerate application performance for files, email, Web, SSL, and rich media applications.
- Significantly reduce bandwidth with leading compression, byte caching and object caching technologies.
Group Work Area
Is this a viable product?

- Our goal for this project was to determine whether or not a Proxy SG/AV environment would be beneficial for the University of Utah.

- Our recommendations are ultimately based on our own personal opinion of the product as well as the opinions of others who have used it in real production environments.
Web Filter & Proxy Client
Overview of Web Filter

- Comprised of the most frequently accessed sites on the Web, Blue Coat Web Filter runs natively on Blue Coat appliances. The Web Filter solution includes over fifteen million website ratings, representing billions of Web pages, organized into the most relevant and useful categories. To ensure accuracy, each site in the Web Filter database is classified into multiple categories, as appropriate. This allows Web Filter customers to define a virtually unlimited number of “cross-categories” to fit their specific filtering requirements.

- Web Pulse uses Dynamic Link Analysis (DLA) to check popular Web sites for attack injections and search engine results for bait pages, both leading to Web threats via dynamic links. Web Pulse has eight operation centers to support cloud defense analysis of more than 2 billion Web requests per week.
Benefits of Web Filter

- Block specific types of student web traffic based on predetermined website categories. (Gambling, Porn, Social Networking etc.)
- Allows network administrators to limit students to more "productive" websites.
- Cuts down on wasteful bandwidth use which frees up more network speed for the rest of the university.
Web Filter Control Panel

Allows administrators to implicitly or explicitly deny all web traffic based upon website categories.
Proxy SG allows administrators to implement Bluecoat's proprietary Web Filter database in addition to several 3rd party databases.
Web Filter database is automatically updated regularly by connecting to Blue Coat's **Web Pulse** cloud service.
Blue Coat Proxy Client helps deliver a headquarters work experience to all employees wherever they are. With Proxy Client, you can define which applications to accelerate and which to block based on security and bandwidth requirements. Proxy Client is administered with the Proxy SG management console for easy provisioning, configuration and maintenance. It can also be distributed to end-user machines using standard software provisioning services and is automatically updated to minimize ongoing administrative time and resources.
Proxy Client software installed on client machines allows Web Filter to "push" administrator filter settings to end users.
Users attempting to access forbidden content are now prevented from doing so. Administrators can create custom deny/warning screens to suit their needs.
Web Filter Demo
Bandwidth Management
Bandwidth management allows you to classify, control, and limit the amount of bandwidth used by different classes of network traffic flowing into or out of the Proxy SG appliance.

Accomplishes any of the following:

- Guarantee that certain bandwidth classes receive a specified minimum amount of available bandwidth
- Limit certain traffic classes to a specified maximum amount of bandwidth
- Prioritize certain traffic classes to determine which classes have priority over available bandwidth
Some examples...

- Ensure that the company CEO is guaranteed the highest level of service on the network.
- Ensure that Citrix ICA traffic is always given a higher priority than HTTP.
- Establish that resource hogging services, like video streaming, are given a specified maximum amount of bandwidth.
- If a user is identified as using a p2p service, throttle his/her bandwidth.
Some examples...

- Ensure that the company CEO is guaranteed the highest level of service on the network.
- Ensure that Citrix ICA traffic is always given a higher priority than HTTP.
- Establish that resource hogging services, like video streaming, are given a specified maximum amount of bandwidth.
- If a user is identified as using a p2p service, throttle his/her bandwidth.
2011 Estimates

- Total online viewership during work hours is likely to reach at least 8.4 million hours.
- Average hourly earnings: $22.87
- Total financial impact: > $192 million

Compared to how many hours are worked in total for the length of the tournament (11 billion), the hours lost are only a drop in the bucket. However, the danger is not in lost man hours, but the bandwidth strain on the companies network, which can lead to serious productivity issues.

"The situation is comparable to a traffic accident, which does not have an measurable impact on the overall economy, but if you happen to be stuck in the resulting congestion and arrive late to work because of it, it has an immediate and noticeable impact on your days productivity"
Solution: Create a policy that limits the amount of bandwidth that can be used for TV/Video streaming services during the three weeks of the tournament.

1. Create a bandwidth management class
2. Create a new web access layer
3. Set a new destination object (TV/Video Streams)
4. Set action object (server-side, inbound)
5. Set a time object
6. Install policy and test
Create a Bandwidth Management Class
Create a New Web Access Layer

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Time</th>
<th>Action</th>
<th>Track</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Set a New Destination Object

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Time</th>
<th>Action</th>
<th>Track</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Edit Request URL Category Object**

- **Name**: TV/Video Streams
- **Categories**:
  - Spyware Effects/Privacy Concerns
  - Spyware/Malware Sources
  - Suspicious
  - TV/Video Streams
  - Tobacco
  - Translation
  - Travel
  - Vehicles
  - Violence/Hate/Racism
  - Weapons

- **Selected Categories**: TV/Video Streams
Set an Action Object
Set a Time Object

Add Time Object

- Name: MM_Time
- Use Local Time Zone
- Use UTC Time Zone
  - Only between the following times of day:
    - From: 00:00
    - To: 23:59
  - Only on the following days of the week:
    - Enable
    - Monday
    - Tuesday
    - Wednesday
    - Thursday
    - Friday
    - Saturday
    - Sunday
  - Only between the following days of the month (inclusive):
    - From: 01
    - To: 01
  - Only between the following dates of the year (inclusive):
    - From: March 15
    - To: April 04
  - Only between the following dates (inclusive):
    - From: 2011 January 01
    - To: 2011 January 01

OK  Cancel  Help
Install Policy

Policy Installed

Policy installation was successful

OK

Settings retrieved from SG Appliance 155.97.61.143
## Review Statistics

### Current Class Statistics

<table>
<thead>
<tr>
<th>Bandwidth Class</th>
<th>Current Packet Rate (pps)</th>
<th>Current Bandwidth (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPI_EWMA</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Bandwidth Management Demo
Proxy Services
Benefits...

- Block protocols like Telnet, FTP, SSH and more
- Block specific IP addresses, ports, and subnet ranges
  - Black hole the IP addresses of attackers
- Create static bypass lists
- Create restricted intercept lists
Block potentially dangerous protocols
- Create new service groups and block services

Block specific IP addresses, ports, and subnet ranges
Specify clients or servers, by IP address, that can bypass the Proxy SG
Restrict packet interception, by IP address, to specific clients or servers
Proxy Services Demo
Application Delivery Network
Application Delivery Network focuses on delivering network applications and resources quickly and efficiently across a WAN setup.

ADN Manager is responsible for publishing the routes to other clients and peer devices on the ADN network.

Uses compression and secure communications to accomplish fast and secure delivery of applications across WAN.

Allows for secure communication through appliance certificates.
The ADN network is usually comprised of a

- Manager (Manages the ADN network policies and network)
- Backup manager (Takes over for the manager when it is not available)
- ADN nodes (Devices connected on remote LANs to communicate with the manager)
- Proper configuration

The backup manager is not necessary. However, failure to implement a backup appliance will result in loss of network ADN connectivity should the primary manager ever go down.
Faster and more secure delivery of internal applications to satellite locations of a company’s WAN where larger applications like CRM, accounting management, etc. are likely to be used on a frequent basis.

Speed of delivery is top priority for ADN. This is mainly accomplished through byte caching of data, even encrypted data!
Define ADN manager

Assign ADN proxy to the subnet to which it will preside

Approve any Peer ADN node proxies that will be connected to the manager for updates to policies

Define Tunneling protocols and ports if needed

Most options can be left as default
ADN Setup (Client)

- Install the Blue Coat Client app

- The client should automatically gain the benefits of ADN functionality once it “sees” the ADN server it is supposed to be connected to on its network segment
The “Total Savings” and “Savings Over Time” tabs report the bandwidth savings gained as a result of having the ADN functionality enabled.
ADN setup is as simple as defining the primary ADN manager of the network then setting up the network to which the manager is assigned.
ADN Peers

- Allow for WAN segments of companies to gain the benefits of ADN proxy managed from one location by connecting to the ADN manager with a “lesser” peer proxy server.

- This peer is sent updates on a regular basis from the manager, similar to a domain controller to domain added computers.
Reverse Proxy
Server Accelerator

- Reverse Proxy acts as a server accelerator by reducing response time to client requests
- It’s very easy to scale out a deployment utilizing reverse proxy from the origin content server
- Acts as if it is the origin content server
Proxy Acceleration Profile

- Determines object caching and pipelining behavior
- Predefined attributes are setup to meet a specific objective.
- **The core objectives are:**
  1) Reduce response time for clients,
  2) Reduce load on the origin server, and
  3) Reduce server-side bandwidth usage.
University Hospital

Competitive Analysis
Use Case

- Multiple Blue Coat Appliances
Setup

- Blue Coat Proxy SG Appliances
- Web filtering
- Reverse proxy caching
- No bandwidth management
Application speed and response

Benefits

- Low price based on the whole gamut of features
- Web filtering protects internal network
- Internal application speed and responsiveness improved
Vendors will mislead you

**Issues**

- Proxy SG appliance unable to manage bandwidth due to lack of machine resources
- Do not trust vendor implementation and integration claims
- None of the services really stand out – very similar to other products
Mormon.org

Competitive Analysis
Use Case

- Two Proxy SG 9000 Series
- Three SG 8000 Series
Setup

- Blue Coat Proxy SG Appliances are used exclusively in a reverse proxy configuration.
- It is a hybrid solution with F5 load balancers and original content servers.
- All content on the site is cached onto the Proxy SG Appliances.
Configuration
Benefits

- Allows for flexible horizontal scaling and traffic management.
- Protects original content servers from attacks
- Fast and responsive web applications
Issues

- High cost of ownership and maintenance
- SGOS version limitations
- Customer support
- Poor reporting
Is this a viable product?
School Statistics

- ~31000 attending students
- 15/1 ratio of faculty to students: ~2000 faculty
- ~20 colleges
- Estimated simultaneous connections at any given time: >100,000

- Blue Coat Proxy SG 9000 – 40 stock
  Unlimited employee licensing
  Recommended connection maximum – 100,000
2x ProxySG 9000 – 40 : load balanced
Recommended uses

- All-in-one enterprise solution for **WAN optimization and web filtering**
- Content and application delivery acceleration through caching
- Scale and safeguard original content servers
Concerns

You’ve been warned

- Open source alternate solutions available
- Most features will not be deployed
- Significant time investment to configure
- Horrible and expensive customer service
- Current users looking for new solutions
- Costly to deploy and maintain
Market Leader in Web Filtering

Lessons learned

- Blue Coat Web filtering is the market leader and extremely effective. Web Pulse cloud updates. Simple interface and setup.
- Proxy services are widely used and efficient
- Bandwidth management is effective only if the hardware can supports it
- ADN is effective for increasing speed and application performance.
Multi Function Products

Web Filtering and Reverse Proxy

- Multi function products tend to get utilized for one or two things
- When implementing Blue Coat products into production environments not all functions are useable
- Be very cautious about testing and impact to your production environment
Enterprise Networks

- Need formal implementation and test process. Lack of detailed implementation documentation.

- We gained valuable knowledge that translates into other fields and increases our overall marketability.
Questions?