Blue Coat® Systems

Secure Web Gateway Deployment Methodologies

Blue Coat®

Americas:

Blue Coat Systems, Inc.
420 N. Mary Ave.
Sunnyvale, CA 94085

Rest of the World:

Blue Coat Systems International SARL
3a Route des Arsenaux
1700 Fribourg, Switzerland

Document History

Date	Version	Note
January 15, 2013	v1.0	Initial release

Contents

Introduction

As the Internet has become a critical part of most organizations' infrastructure, it is important to select a Secure Web Gateway deployment method that will best serve your business needs, while taking into account network topologies and levels of end-point control.

This document discusses the three most common deployment methods for a physical appliance. Customers should also consider whether physical appliances or alternative options, such as Cloud and/or Virtualized Secure Web Gateways, would best suit their needs; however those alternative options go beyond the scope of this document.

Secure Web Gateway deployments typically involve some or all of the following components:

- Physical installation
- Authentication
- Policy and Content Filtering
- Anti-Malware scanning
- Logging
- Reporting
- Management

Each of these aspects should be considered prior to selecting a deployment method. For instance, a physically inline deployment might not be the best option if you have multiple paths to the Internet and you want to provide gateway anti-malware scanning using the ProxyAV appliance.

The three most commonly used deployment scenarios for appliance-based solutions are:

- Physically Inline (Transparent)
- Out-of-Path or Virtually Inline (Transparent)
- Explicit

The subsequent sections in this document describe the differences between these deployment options, and the advantages and disadvantages associated with each.

Scenario

Physically Inline Deployment (Transparent)

A physically inline deployment utilizes the ProxySG appliance bridge (passthrough) card, which typically bridges the connection between a core/distribution switch and the WAN router. (See Figure 1–1.)

Figure 1–1 Physically inline deployment

With a physically inline deployment, the users' browsers are not typically aware that there is a proxy in the network, and requests are sent directly to the Origin Content Server (OCS). The ProxySG appliance is then configured to transparently intercept this traffic, which could include HTTP, HTTPS, FTP, etc.

Because all traffic destined for the Internet transits the ProxySG appliance, certain traffic may need to be bypassed using the Proxy Service rules. When traffic is intercepted, the ProxySG appliance terminates the request from the client and establishes a new outbound connection to the OCS to retrieve the requested data.

When the ProxySG appliance is installed physically inline, it's possible to reflect the original client source IP address as the request transits the ProxySG appliance, or use the ProxySG appliance's IP address as the source when the request is made to the server. Using the ProxySG appliance IP address as the source is typically more desirable, as this can be defined as the only IP address on the firewall that is allowed to make outbound requests to port 80 or 443, for example.

Physically Inline Deployment Advantages

A physically inline deployment is the simplest method to deploy, because it does not require any end-user browser configuration, and it guarantees that all Web traffic will be intercepted and flow through the gateway. It is also considered secure, as there is no chance of a user bypassing end-user controls set by the administrator, as long as it is the only path available to the Internet.

Physically inline is a good option if an organization has a number of applications that need to access the Internet that are not proxy aware. With a physically inline device, there is no need to specify any ProxySG appliance settings for these applications.

Another advantage is the ability to monitor all ports for call home traffic generated by malware and botnets from infected computers. This awareness allows for remediation of infected systems, thus lowering the risks of Web access for an organization.

Physically Inline Deployment Disadvantages

While a physically inline installation simplifies certain aspects of the deployment, there are also a number of disadvantages to using this method.

- It is harder to achieve resiliency using a physically inline deployment. It is possible to daisy chain devices in serial, but this complicates the deployment as failover groups are required, and most organizations do not like the concept of multiple devices installed in the path of the traffic.

- If an inline ProxySG appliance fails, the passthrough card can be configured to fail open or fail closed.
  - Failing open allows the link between the switch and the router to remain up, so traffic can still flow in and out of the network (depending on firewall rules).
  - Failing closed breaks the link between the switch and router, which is often useful if there is a second ProxySG appliance and path available to the Internet.
- Authentication is also more complex in a transparent proxy environment. When using explicit proxy, the browser knows there is a proxy in the path and therefore, the proxy can use an HTTP 407 "Proxy authentication required" challenge to request that the end-user or browser sends the authentication credentials. However in a transparent environment, the browser is not aware of the ProxySG appliance and therefore, can only be sent an HTTP 401 "authentication required" challenge. A 401 challenge is normally sent from the OCS to the end user/browser. To achieve this, the transparent proxy has to redirect an incoming request to a virtual URL, which is used to replicate an OCS to generate the 401 challenge, so that the end user can send the authentication credentials.
- Installing a ProxySG appliance physically inline adds an overhead, because the ProxySG appliance has to look at all traffic as it transits the bridge card to determine whether the traffic should be intercepted or bypassed. Therefore, this overhead needs to be considered when the ProxySG appliance is sized.

Virtually Inline Deployment (Transparent)

A Virtually Inline Transparent deployment allows a Web gateway to be deployed in any network location that has connectivity, similarly to an explicit mode deployment. A redirection mechanism such as WCCP or Policy Based Routing (PBR) is then used to redirect interesting traffic, such as HTTP and HTTPS to the ProxySG appliance. (See Figure 1–2.)

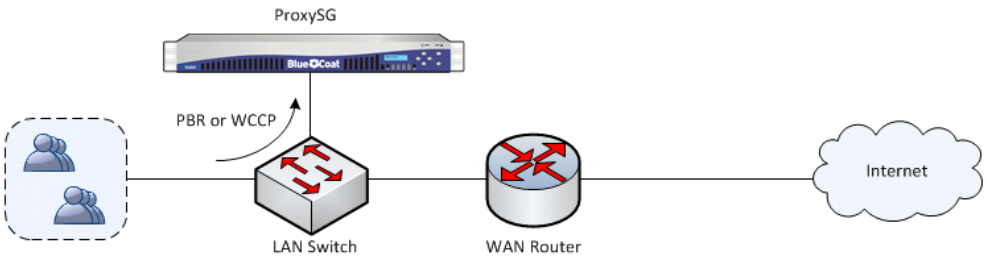

Figure 1–2 Virtually inline deployment

This method is typically used when transparent proxy is required, but a physically inline deployment is not possible, such as when the network capacity is too large, or simple resiliency is required.

Virtually Inline Deployment Advantages

The advantages to a Virtually Inline transparent deployment are similar to those of the physically inline deployment.

- The administration overhead is low, as no end-user browser changes are required. Assuming that the redirection mechanism is configured correctly, it should be impossible for end-users to bypass the proxy.
- A virtually inline deployment also simplifies resiliency and can provide load sharing if using a protocol such as WCCP. WCCP natively provides load balancing and failure detection, ensuring that the service remains active in the event of a ProxySG appliance failure.
- Unlike a physically inline deployment, a virtually inline device will only be sent the traffic that it needs to proxy and therefore the overall size of the link is not a limiting factor, and there is no overhead on the device to process traffic that is not going to be proxied.
- The need to redirect return traffic from the Web server can be negated by sending the Proxy IP address as the request leaves the ProxySG appliance, ensuring that all return traffic is sent directly back to the ProxySG appliance.

Virtually Inline Deployment Disadvantages

The main disadvantages to a Virtually Inline deployment are the availability of the redirection mechanisms and the additional level of complexity they add.

- If you are using WCCP, the router or switch will obviously need to support WCCP and be running the correct software version. In addition, WCCP also creates additional load on the switch or router, particularly when using GRE as opposed to L2 forwarding. For this reason, L2 is the preferred method for forward and return of traffic between the router and ProxySG appliance; however, this can only be used if both devices are in the same broadcast domain.
- While the WCCP configuration can be relatively simple in a basic network topology, it can become more complex when configured in larger networks that have resilient connections and multiple VLANs.
- As this is a transparent proxy deployment, much like the physically inline deployment, the same complications exist with authentication, whereby a virtual URL redirect is required to send the HTTP 401 challenge to the browser.

Explicit Deployment

Explicit deployment is the most common Proxy installation method, which allows for the ProxySG appliance to be installed out of path while simultaneously providing resiliency, load balancing, and excellent scaling capabilities. To facilitate this kind of deployment, an administrator can distribute PAC files to explicitly point the end-users' browsers to the ProxySG appliance.

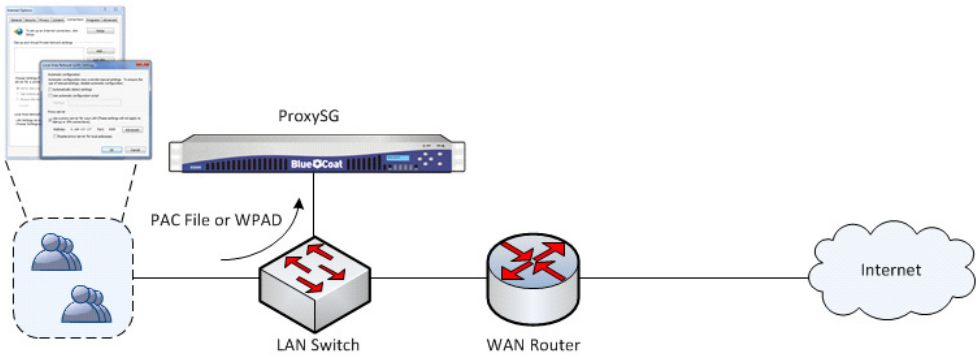

Figure 1–3 Explicit deployment

When using an explicit deployment, it is extremely important to have the firewall properly configured to prevent users from bypassing the proxy. This is especially important if users have administrative rights to their computer and are able to remove proxy settings. The firewall needs to be configured to only allow the proxy to talk through the firewall using HTTP and HTTPS. All other hosts/ IP addresses should be denied.

Explicit Mode Advantages

Explicit proxy enables organizations to deploy a Secure Web Gateway without any disruption or changes to the network. The Secure Web Gateway can be installed using a single switch port connection, and scaling and resiliency can be provided horizontally, with the PAC file distributing traffic across multiple devices.

Using Blue Coat's iteration of VRRP (SGRP), high availability and load balancing can be achieved through the use of a PAC file and DNS. This method utilizes VIPs and the ProxySG appliances work together as master and slave. Using multiple VIPS for each device allows a single device to be a master for one VIP and slave for the other. If these VIPS are both put into DNS, traffic can be load-shared and resiliency is automatically provided if one ProxySG appliance fails.

Authentication is much simpler using Explicit proxy, with the browser able to accept authentication challenges directly from the Secure Web Gateway as opposed to the OCS with transparent proxy, there is no requirement to perform redirects to a virtual URL

Explicit Mode Disadvantages

The disadvantage of an explicit mode deployment is the increased administrative overhead, because each client device needs the proxy settings defined so that traffic is sent to the proxy.

While there is some reduction in this overhead with PAC and WPAD, any error in configuration of an end-user system will result in a help desk call and require a system administrator to rectify the situation. Explicit mode deployment also relies

heavily on a properly configured network and firewall. Any hole in the network or firewall can be exploited by a knowledgeable end-user to bypass the Web gateway, as discussed earlier.

For call home traffic analysis, port monitoring needs to be done by a network device with access to all egress-point network traffic. The explicit mode Web gateway can detect and block call home traffic only for protocols defined and managed, such as HTTP and HTTPS.

Conclusion

This document is not designed to recommend a specific deployment method. When determining the most appropriate method to use, each of the advantages and disadvantages for the various different deployment methods should be evaluated with your own security and network requirements in mind.

In addition to this document, your local Blue Coat Systems Engineer can work with you to understand your requirements and suggest the most appropriate deployment method to meet your needs.

About Technical Briefs

Technical briefs are designed to illustrate the features and capabilities of Blue Coat products. By describing generic solutions, technical briefs provide a foundation that Blue Coat customers can use to understand how Blue Coat products can be used to solve specific problems.

These technical briefs are not intended to solve customer-specific requests; if you need a customized solution to address a specific concern, contact Blue Coat Professional Services at professional-services@bluecoat.com.