Network
+ Security
+ Cloud

SECURE WEB GATEWAY DEPLOYMENT METHODOLOGIES

In today's complex network architectures it seems there are limitless ways to deploy networking equipment. This may be the case for some networking gear, but for web gateways there are only a few proven deployment methodologies that are effective and provide complete security.

In this article, we'll talk about the four most common types of web gateway network deployments. Sometimes referred to as forward proxies, these devices are used to secure web access for an organization's internal end-users. The four commonly used deployment scenarios for web gateways are inline, explicit, transparent and SPAN port. Each one of these deployments has its advantages and disadvantages.

Inline Deployment

Inline deployment is the simplest and easiest to describe. Smaller deployments, such as a branch office, will typically use an inline deployment due to the ease of deployment and the absolute security level it provides.

With an inline deployment, the web gateway is placed directly in the path of all network traffic going to and from the Internet (Figure 1). If you choose an inline deployment, make sure your web gateway is capable of bypassing network traffic that you don't want processed by the web gateway. In many instances, you can choose to either "proxy" (re-route) or"bypass" a specific protocol. If you "proxy" the protocol, it means the web gateway will terminate the traffic from the client to the server locally, and re-establish a new connection acting as the client to the server to get the requested information.

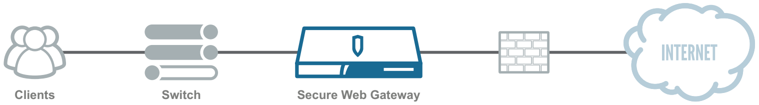

Figure 1 - Inline Deployment

Inline Deployment Advantages

The upside of an inline methodology is the ease of deployment and the guaranteed assurance that all web traffic will be re-routed to flow through the gateway. There is no chance of a user bypassing the controls set by the administrator as long as the device is inline and is the only path available to the Internet. All Internet bound HTTP traffic will be processed and handled by the web gateway. Another advantage is the ability to monitor all ports for call home traffic generated by malware and botnets on infected computers. This awareness allows for remediation of infected systems lowering the risks of web access for an organization.

Inline Deployment Disadvantages

The disadvantage of an inline deployment is a single point of failure. Even with technologies like "fail to wire", which allows all traffic to flow through when a device fails, many organizations are uncomfortable with a single device in the data stream to the Internet. Although unlikely, a partial failure of the device could result in a small outage. For a small organization or a branch office a short disruption may not be an urgent concern, but for a larger organization Internet access can be mission critical.

Another disadvantage (really a side effect of this being the most secure deployment methodology), is that with inline deployment there is the necessity to manage all the protocols proxied by the web gateway. Because the web gateway is inline, all other protocols (FTP, CIFS, etc) that will need to be proxied or bypassed by the web gateway. The IT admin will need to administer this list and the handling of each protocol used by the organization. This adds the highest level of security for an organization.

Explicit Deployment

Explicit deployment is commonly used when a web gateway is deployed in a larger network, and the design of the network requires there to be no single point of failure. Explicit deployment allows the web gateway to be located on the network in any location that is accessible by all users and the device itself has access to the Internet (Figure 2). Explicit deployment uses an explicit definition in a web browser. To facilitate this kind of deployment an administrator can distribute PAC or WPAD files for the explicit proxy setup in end-user browsers.

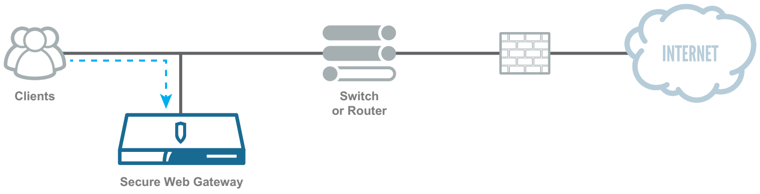

Figure 2 - Explicit Deployment
Client has an explicitly defined proxy in its settings for the web browser

When using explicit deployment it is extremely important to have the firewall properly configured to prevent users from bypassing the proxy. The firewall needs to be configured to allow only the proxy to talk through the firewall using HTTP and HTTPS. All other hosts/IP addresses should be denied. In addition, all other ports need to be locked down to prevent end-users from setting up their own proxy internally that tries to access the Internet via HTTP on a port other than the commonly used ones (80 and 443).

Explicit Mode Advantages

The main advantages of deploying a web gateway in explicit mode include narrowing the amount of traffic processed by the web gateway (you can limit traffic to only HTTP based traffic), and the ability to more easily implement redundancy for web gateways in your environment. Explicit mode deployment for an environment without an existing web gateway is also less disruptive to the network. The web gateway can be placed anywhere in the network that is accessible by all end-users as long as the web gateway is able to reach the Internet.

Explicit Mode Disadvantages

The disadvantage of explicit mode deployment involves IT administrative overhead as each client station needs a configuration change in order to work properly. 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 helpdesk call and require a sysadmin 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. Also, 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.

Transparent Deployment

Transparent deployment allows a web gateway to be deployed in any network location that has connectivity, similarly to explicit mode deployment (Figure 3), reducing the need for a configuration change to the network to implement. In addition, there is no administrative overhead to configure end-user systems, since the routing of HTTP and HTTPS traffic is typically done by the router or other network device. Transparent deployment is often used when an organization is too large for an inline deployment and does not want the added work and overhead needed for an explicit deployment. Most transparent deployments rely on web Caching Communications Protocol (WCCP), a protocol supported by many network devices. Alternatively transparent deployment can be achieved using Policy Based Routing (PBR).

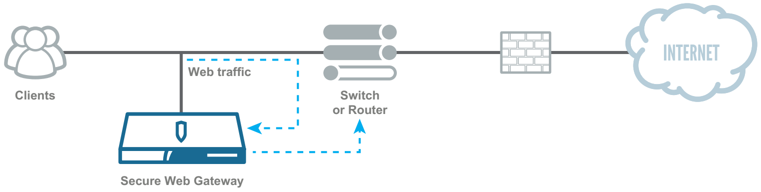

Figure 3 - Transparent Deployment
Router and SWG use WCCP for communications

Transparent Deployment Advantages

The main advantages of deploying a web gateway in transparent mode include narrowing the amount of traffic processed by the proxy, and the ability to more easily implement redundancy of the web gateway. In addition, transparent deployment does not require changes to end-user systems.

Transparent Deployment Disadvantages

Transparent deployment does depend on the availability of either WCCP or PBR, and support for these by the web gateway, typically available only on more sophisticated web gateways. Configuration can be trickier as there needs to be compatibility of supported versions of WCCP between the router and the web gateway. More in-depth network expertise is required to implement and deploy a transparent mode deployment, which may not be a problem in larger organizations but could be an issue for smaller organizations.

SPAN Port Deployment

The last deployment methodology is the SPAN (Switched Port Analyzer) port deployment. Sometimes this method is called TCP Reset deployment, as it relies on TCP resets to implement the policy of the web gateway. A web gateway is deployed by attaching it to a SPAN port on a switch (Figure 4). Unlike the other three deployment methods, which process the web traffic and implement policies based on the network response the web gateway issues, a web gateway deployed on a SPAN port implements policies by issuing a TCP reset to the client system to prevent completing a download of offending content.

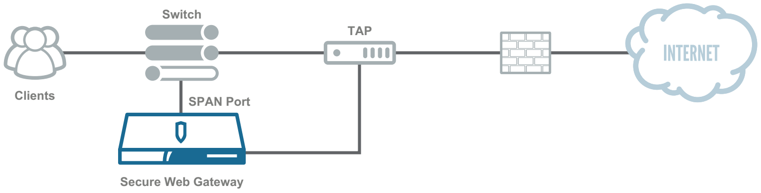

Figure 4 - SPAN Port Deployment

SPAN Port Advantages

SPAN port deployments are advantageous for large scale deployments because the monitoring mode typically uses fewer resources than inline, explicit or transparent, which all must actively process traffic. A SPAN port deployment is useful if you think your hardware might be undersized for your needs. Finally, port monitoring to passively detect call home attempts on most ports and network traffic is available with this deployment method.

SPAN Port Disadvantages

A SPAN port deployment on a switch does not see all the traffic. Corrupt network packets, packets below minimum size, and layer 1 and 2 errors are usually dropped by the switch. In addition, it's possible a SPAN port can introduce network delays. The software architecture of low-end switches introduces delay by copying the spanned packets. Also, if the data is being aggregated through a gigabit fiber optic port, a delay is introduced as the signal is converted from electrical to optical. Any network delay can be critical since TCP resets are used to implement policy.

SPAN ports also have an issue when there is an overload of traffic. Typically the port will drop packets and result in some data loss. In a high network load situation most web gateways connected to a SPAN port will not be able to respond quickly enough to keep malware from spreading across a corporate network.

Recently a Network World article (Dec 7, 2009) discussed the TCP reset method used by web gateways to implement policy:

> **Too clever by half, perhaps –TCP RESET has several drawbacks.**
>
> *First, a cyber attacker can cause a "self-inflicted DoS attack" by flooding your network with thousands of offending packets. The TCP RESET gateway responds by issuing two TCP RESETs for every offending packet it sees.*
>
> *The TCP RESET approach is worthless against a cyber attacker who uses UDP to "phone home" the contents of your sensitive files.*
>
> *The gateway has to be perfectly quick; it has to send the TCP RESET packets before the client (victim) has processed the final packet of malware.*
>
> *Ergo – deep and thorough inspection of network traffic before it's allowed to flow to the client is the most effective way to stop malware.*
>
> *...In other words, don't just wave at the malware as it goes by.*
>
> **–Barry Nance, Network World, Dec 7, 2009**

Finally, a SPAN port deployment monitors traffic passively. A web gateway with inline, explicit or transparent deployments will stop network traffic allowing for real-time ratings, cloud intelligence requests in hybrid web gateway architectures, data loss prevention checks on out going traffic, re-writes of web request and response variables, deep inspection of compressed archives and data transfers and optimization of web content delivery via caching, stream splitting and bandwidth management.

Conclusion

While there are four common deployment methodologies to choose from when implementing a secure web gateway, there are really only three clear common choices for IT departments. The choice between inline, explicit and transparent, will have to be done based on the needs and resources of the organization and the IT department. Even though SPAN port deployment with TCP reset may seem like a reasonable solution, there are sufficient drawbacks that a serious web gateway deployment should avoid this methodology.

BLUE COAT®

Network
+ Security
+ Cloud

v.WP-SWG-DEPLOYMENT-METHODOLOGIES-EN-v2c-0216

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000