WHITE PAPER

Transparent v. Proxy Mode

WHICH SHOULD YOU CHOOSE?

ComSifter®
protect web users now!

Article Update: January 2013

IN THIS DOCUMENT

- History
- Pros and Cons
  Transparent Mode
  Proxy Mode
  Which is the right solution for our network?
- Background Information
  Transparent Mode
  Proxy Mode
- Proxy Configuration for Various Browsers
  Internet Explorer on a local Machine
  Internet Explorer on a local machine using a Local Group Policy
  Internet Explorer on a Domain Network using a Domain Group Policy
  Other Browsers
  Safari on a local machine
- Contacting the ComSifter with a Browser in Proxy Mode

HISTORY

Occasionally, Comsift receives reports that the filter is being bypassed, especially with social networking sites such as Facebook. The reports state that the user can simply put an "s" in the address bar so the header reads HTTPS as opposed to HTTP. Additionally, there are reports that some secure transaction do not complete. Both of these conditions are solved by configuring the browser (Internet Explorer, Firefox, Safari, etc.) to use proxy mode. Placing the browser in proxy mode will offer better compatibility and a more secure networking environment.

When initially configuring your ComSifter it is important to understand the concepts of transparent and proxy modes.

PROS AND CONS

Transparent Mode

PRO » Does not require any browser configuration.

CON » HTTPS transactions may fail as the ComSifter may be seen as a man-in-the-middle.

» Encrypted traffic may be used to access web sites—the ComSifter is not able to see the data.

Proxy Mode

PRO » HTTPS transactions work properly as ComSifter is not seen as a man-in-the-middle.

» ComSifter has a chance to see if a site is on the blacklist before it becomes encrypted.

CON » Requires browser setup

» May interfere with server packages (WSUS, Exchange, etc.), anti-virus software updates, etc., and will require entering the proxy information into these programs. (Newer programs follow the Proxy settings used in Internet Explorer, making this less of an issue)

Which is the right solution for our network?

Proxy mode is always the preferred setup. It is more robust—especially with HTTPS transactions, and gives the network administrator much greater control over what client applications can access the Internet.

Exceptions to this would be:

- Use of the network by very young children (K-6) where HTTPS transactions would not be used.
- Situations where the ComSifter is used in a whitelist mode—and all whitelisted sites are known to work.
- Situations were the Internet curriculum is fixed and all sites are known to work properly.

CONTINUED

BACKGROUND INFORMATION

Unlike a router, that only has to pass packets to and from the LAN to the Internet, the ComSifter must retrieve all of a page. The page you view in your browser consists of many connects—as few as two, as many as a few hundred—that are assembled by the browser and presented as a finished page. The ComSifter cannot display any of the page until it has all of the page as the last connect could be, or could point to, objectionable content.

When the ComSifter is retrieving a page from a website, it is doing so as a result of a request from a client computer. When doing this, the ComSifter is acting as a proxy for the client computer making the request. It is at this point where the differences between transparent and proxy mode become important.

Transparent Mode

In transparent mode, the browser makes a request to retrieve a page from a web site. This request is made using the HTTP protocol and is made using standard port 80. The ComSifter intercepts this request and retrieves the page from the web site, applies the appropriate filter rules and then gives the requesting computer the complete page or a denied page. All of this is done transparently and requires no special configuration of the browser.

In most cases, this procedure works as expected, but there are instances when it will fail. Some websites have instituted very strict man-in-the-middle detection schemes. Typically, these sites are involved with secure (HTTPS) transactions with the client computer and they must protect themselves from man-in-the-middle fraud schemes. In certain instances, the security schemes of these sites determine that the ComSifter is a man-in-the-middle and refuse to complete the transaction.

Additionally, if a client program uses a non-standard port (not port 80) and encrypts the transmission (HTTPS) the ComSifter is unable to see the data and apply filtering rules. The real world result of this is users are able to try adding an “s” to the protocol (HTTPS) to see if the web site has a secure server. If so, this will circumvent the filter.

Proxy Mode

All modern browsers (Internet Explorer, Firefox, Safari, etc) have a proxy mode. In this mode the browser changes how it makes a request for a web page. Devices in the path to the website (such as the ComSifter) are then able to identify themselves to the website that they are a proxy and are acting at the request of the client. Websites see this as a legitimate request and allow secure transactions to complete (that may have failed if in transparent mode). Proxy operation is typically more robust than transparent mode but does require the extra step of changing the browser to proxy mode (this is mitigated if the network is part of a domain and under control of Group Policies. Proxy mode may be easily set up under Group Policies.)

An added benefit of proxy mode is that it gives network administrators much more control over what goes out to the Internet. In transparent mode, all ports are active and available for use by the client computer (64,000 ports). If a client program uses a non-standard port (not port 80) and encrypts the transmission (HTTPS) the ComSifter is unable to see the data and apply filtering rules. In proxy mode, all client requests are made over port 8080. The client asks for a “connect” to the website and also requests a port number. This is all done in the clear (not encrypted). The ComSifter is then able to see the requested website and determine if it is on a blacklist. If so, the page is denied—if not, the ComSifter honors the browsers request for a port at which time the browser encrypts the data and the ComSifter is no longer able to see the data.

PROXY CONFIGURATION FOR VARIOUS BROWSERS

Internet Explorer 6–8 on a local Machine

1. Open Internet Explorer
2. Click on "Tools" menu
3. Click on "Internet Options"
4. Click on the tab that says "Connections"
5. Click on "LAN settings"
6. Under the "Proxy Setting" title, place a check in the box that says, "Use a proxy server for your LAN."
7. In the "Address Field," enter the IP of the ComSifter (e.g., 192.168.1.9).
8. In the "Port Field," enter 8080.
9. Click "OK"
10. 1Close and re-open the browser.

The browser is now in Proxy Mode.

Internet Explorer 6–8 on a local machine using a Local Group Policy

1. Log into the computer using an account that has administrative privileges.
2. Open the Start menu and click on "Run"
3. In the text field, enter "gpedit.msc". This should open the local machine Local Group Policy Editor
4. In the left panel, expand "User Configuration"
5. Expand "Windows Settings"
6. Expand "Internet Explorer Maintenance"
7. Click on "Connection"
8. In the right panel double-click on "Proxy Settings"
9. In the new Proxy Settings window click on "Enable proxy settings"
10. 1In the "Address of proxy" field enter the ComSifter's IP (e.g., 192.168.1.9) and enter 8080 in the "Port" field.
11. Click OK

The browser is now in Proxy Mode.

> Note: It is a good practice to disable the ability of the user to change the proxy setting locally as described above. This may be accomplished by disabling the Internet Tools Connection page. While in the Local Group Policy this may be accomplished by:
>
> 1. Expand "Computer Configuration" in the left pane
> 2. Expand "Administrative Templates"
> 3. Expand "Windows Components"
> 4. Expand "Internet Explorer"
> 5. Click on "Internet Control Panel"
> 6. In the right panel, double-click "Disable the Connection Page".
> 7. In the new window, click on "Enabled" to engage the rule
> 8. Click OK
> 9. Close the Local Group Policy Editor window
>
> The Connections Page will no longer be available to users who do not have administrative privileges.

Internet Explorer 6–8 on a Domain Network using a Domain Group Policy

1. Open the Domain Policy that controls the network.
2. Follow the same steps as outlined above in "Internet Explorer 6-8 on a local machine using a Local Group Policy."
   Note: The above section on disabling the ability to change proxy settings is a best practice for follow for a network environment as well.

Other Browsers
Firefox on a local machine (as of version 3.6)

1. Click on “Tools” menu
2. Click on “Options”
3. Click on “Advanced”
4. Click on the “Network” tab
5. Click on “Settings”
6. Select “Manual proxy configuration” button
7. In the “HTTP Proxy” field enter the ComSifter’s IP (e.g., 192.168.1.9)
8. In the “Port” field, enter 8080.
9. Click OK

The browser is now in Proxy Mode.

Safari on a local machine (as of version 4.05)

1. Click “Edit” menu
2. Click “Preferences”
3. Click the “Advanced” tab
4. Next to “Proxies”, click the “Change Settings…” button
5. Click on “LAN settings”
6. Under the “Proxy server” title, place a check in the box that says, “Use a proxy server for your LAN.”
7. In the “Address” field enter the IP of the ComSifter (e.g., 192.168.1.9).
8. In the “Port” field, enter 8080.
9. Click OK
10. 1Close and re-open the browser.

The browser is now in Proxy Mode.

CONTACTING THE COMSIFTER WITH A BROWSER IN PROXY MODE

Important Note: When proxy mode is enabled in the browser, all traffic is routed through port 8080. Devices on the network that use non-standard ports (not 80) will not be able to be accessed since all traffic is now on 8080—the ComSifter is an example of this situation. It is listening on port 10,000; so trying to access the ComSifter while in proxy mode will fail.

The fix for this issue is very straightforward. All browsers (in the Proxy Configuration area) will have a provision for exceptions. Any IP placed in the exception list will not use Proxy Mode (place the ComSifter’s IP in this exception area).