How to Prevent Secure Web Traffic (HTTPS) from Crippling Your Content Filter

A Cymphonix White Paper

CYMPHONIX

How to Prevent Secure Web Traffic (HTTPS) from Crippling Your Content Filter

Introduction

Internet connectivity is an essential resource for all types of organizations. Utilization of the Internet for research, communications and other mission-critical activity for transacting business, increases daily. Unfortunately, utilization of the Internet for non-critical and detrimental activities outpaces critical activity substantially[1]. This increase of both types of traffic creates a significant challenge for Network Managers; how to limit non-critical and detrimental traffic to ensure mission-critical traffic has the resources it needs.

To complicate the matter, the various traffic types are created by both web browsing activity and application activity. While there are many solutions that address controlling browsing activity, and a few that address application activity, there are very few that handle both well.

Finally, in addition to sorting out mission critical and non-critical traffic generated by both applications and browsing activity, Network Administrators must control the impact of secured browsing traffic. Critical applications are moving to the Internet. Organizations manage contacts with online CRM tools, bank, purchase equipment and perform a myriad of other activities online. Because of the sensitive nature of the data, this type of traffic is often secured. Although encryption provides a tremendous benefit to organizations that want to keep data traveling over the Internet secure, it also adds to the challenge of prioritizing resources for mission critical activity. Because the traffic is encrypted, Network Administrators have no way to determine if the data being transmitted is critical, non-critical or even malicious – creating a virtual "blind spot" in security protection, risk mitigation and Internet usage policy enforcement.

Implications

Resource Management

Network Administrators are held responsible for timely application delivery, whether the application is local, hosted remotely or being served from the Internet. Although bandwidth continues to drop in price and is more readily available, Administrators continue to face overloaded circuits. This occurs most often due to cluttered and un-prioritized Internet data streams – meaning, all users and applications compete for the same resources with little or no prioritization whatsoever. For example, user abuse of encrypted traffic for inappropriate browsing sessions or proxy anonymizing applications can eat up resources that should be used for mission critical activity.

Risk Mitigation

Traffic passing through secured browsing sessions goes unchecked. While this works well for keeping data private, it can be abused by users and sites attempting to infiltrate the network. users that download information over a secured connection prevent spyware and virus scans from verifying the safety of the content. When content is downloaded without these safety precautions, Administrators find their data and overall safety of the network at risk.

Internet Usage Policy Enforcement

In addition to preventing spyware and virus scans, users that download content over secure connections can easily bypass traditional content filtering controls. While all organizations face tremendous risk of litigation for not maintaining "safe" access to the Internet, lack of filtering controls is specifically problematic for educational institutions. Schools must maintain CIPA compliance to qualify for funding and to limit the liability of potentially exposing children to inappropriate material. When gaps result from such at tremendous lack of control, compliance and user safety are lost.
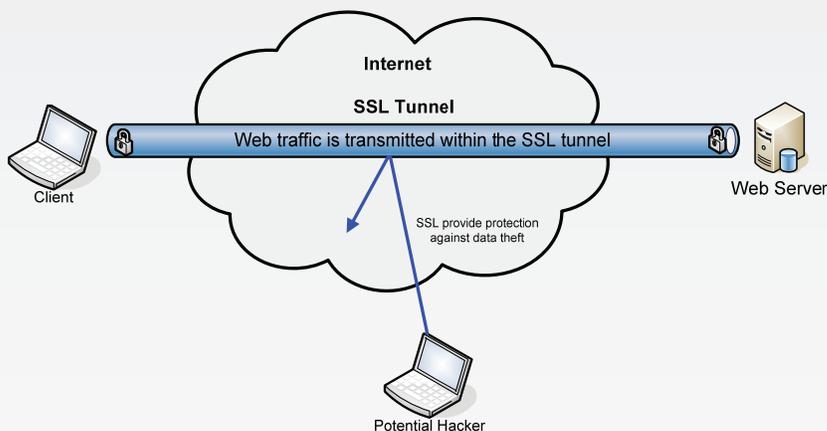
Approaches

Due to the tremendous risks associated with encrypted Internet content, organizations must implement a solution that provides full visibility and control over secure traffic. The new Secure Web traffic visibility feature from Cymphonix allows Network Managers the same visibility and control for secure web traffic as they have for unsecured web traffic. Implementing a solution that addresses both application traffic and secured/unsecured browsing traffic will make it possible for Administrators to maintain Internet usage guidelines across all web traffic.

Secure Web Traffic

The most prevalent form of encryption used is Secure Socket Layer (SSL). SSL allows for a secure tunnel to be established between the user (client) and the web site (server). Secure web traffic is referred to in many ways with the most common being HTTPS and SSL web traffic. HTTPS utilizes SSL encryption to create a secure tunnel between the client and server to transmit website content through the tunnel.
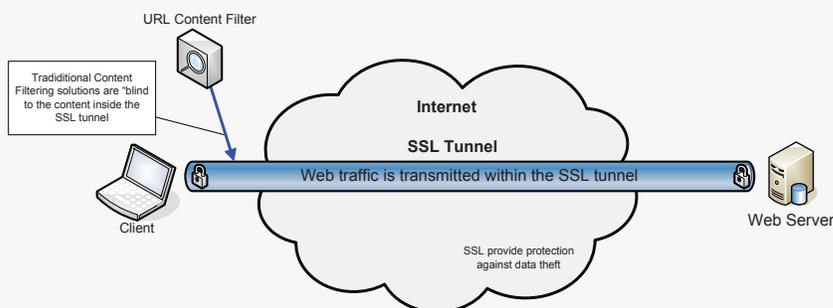
CYMPHONIX

Internet

SSL Tunnel

Web traffic is transmitted within the SSL tunnel

Client

Web Server

SSL provide protection against data theft

Potential Hacker

Why does Secure Web Traffic cause problems?

The benefits of SSL are what cause the problems for traditional content filtering solutions. With an HTTPS web connection the contents of the web traffic are contained within the SSL tunnel and are not visible to the external filtering devices that would normally enforce Internet usage policies.

Traditional web filters are designed to filter based on being able to read URL data. Because HTTPS requests contain only a very limited amount of data (which may be spoofed or inaccurate if provided by an anonymous proxy) relating to the destination and the contents of the request, filters cannot identify the content and are unable to filter.

URL Content Filter

Tradiditional Content Filtering solutions are "blind to the content inside the SSL tunnel

Internet

SSL Tunnel

Web traffic is transmitted within the SSL tunnel

Client

Web Server

SSL provide protection against data theft

SSL Anonymous Proxies

Because it works so well, filter avoidance solutions commonly leverage SSL to allow users to bypass content filters. They do this primarily with three methods; SSL CGI Proxy, SSL Full Proxy and Application-Based networks across SSL – like the Tor Network and Socks 4&5.

SSL CGI Proxy

This type of proxy has the user enter the URL they want to browse into a web form. The CGI script processes the request and fetches the page on behalf of the user. The CGI script changes the links and image references in the web page to point to the URL of the CGI script. All the web requests are going to and from the CGI script so that in most cases URL database categorization cannot be accurately done. All the web requests go to the host of the CGI proxy even if in the original HTML went to many different servers.

Some solutions rely on their maintenance of a database of URL's and IP addresses of these sites to prevent filter subversion. Due to the simplicity of setting up sites to bypass filters in this manner, it is very difficult to keep up with the number of IP addresses and URL's as they can change hourly. Anyone on the Internet with a public IP address can easily setup a proxy like this. There are even Windows versions that can be easily installed on a student's home machine for example – allowing them to use their home computer to bypass the school's content filter while using the school's network. Users can also sign up for mailing lists to receive hundreds of available IP's daily to get around content filters.

Because URL database maintenance works so poorly in this case, the only way to effectively stop this type of inappropriate use is to perform full content analysis. Network Composer's SSL Full Content Filtering allows it to analyze the content of the web site so if an IP or URL is accessed that does not get filtered by the database, it will be filtered by content analysis. Then, if a URL or IP address is not presently found in the Network Composer database, it is sent to Cymphonix automatically to be categorized and added to the URL database. This approach ensures content is filtered regardless of URL or SSL encryption.

SSL Full Proxy

This method requires the user to modify their browser settings to use a proxy server. Since this method requires the user to change their browser settings it is less popular, but nonetheless is a very effective way to bypass content filters. Often, these proxy server sites use non-standard, unchecked port numbers to bypass content filtering. Traditional filters cannot even see the traffic and therefore are unable to filter it.
Because Network Composer identifies application traffic regardless of port or protocol, it can identify web browsing activity and ensures HTTP, HTTPS and

SSL traffic are filtered according to policy.

Application-based Networks across SSL

Tor Network is on example of an SSL based network built to allow users to anonymize their web browsing and bypass content filters. Tor normally uses non standard port numbers to avoid detection, encrypts traffic via SSL connections and can be run from an external memory device such as a UBS thumb drive. This combination of filter avoidance tactics makes it, and applications like it, a very effective way to get around content filters. Even on PCs with application installation controls in place, users can easily run the application from an external device, connect via SSL and browse without controls.

Network Composer is one of the only solutions that can block and control traffic from these types of applications. Because Network Composer includes deep-packet scanning and layer 7 identification capabilities, it can identify these applications and apply policy to prevent the risks associated with them.

SSL Filtering Methods:
SSL Certificate Filtering

This is the most common form of SSL filtering offered by content filtering appliances. This method attempts to validate the host name or CN from the server certificate. Once the host name is obtained it is categorized by a URL database.

Advantages
• A CA certificate does not need to be installed on the client web browser
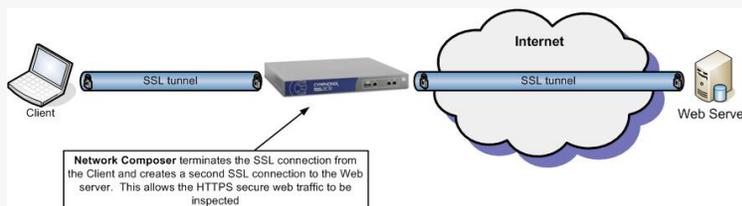• Basic filtering works if the host name is known in the URL database

Disadvantages
• The user cannot be presented with a denied access page. Typically the user will see
the "Page could not be displayed" browser error. The user has no way of knowing
if his page request was blocked by a content filter or because of network
connectivity problems
• Only a URL database check can be done. Since the content of an allowed
connection is encrypted, the HTTP data cannot be used for categorization. This is
specifically problematic with new websites that have not yet been categorized.
• Downloads cannot be scanned for viruses
• Spyware MD5 sum checks cannot be performed
• Spyware Class ID checks cannot be performed
• Streaming media traffic cannot be properly

identified and controlled
• MIME and file types cannot be logged or specifically blocked
• SSL anonymous proxies can be used if the IP or URL is not in the database.

SSL Full Content Filtering

This method is the most robust and complete of the three discussed methods. With this method there is a secure connection between the Network Composer and the user, and a separate secure connection between Network Composer and the server. The Network Composer is acting as an SSL proxy. Because Network Composer can terminate the SSL connection, data can be fully inspected. The Network Composer generates and sends the browser a CA-signed certificate for the host name that was requested. This certificate is installed on the client's browser via a download URL or optionally distributed via Active Directory. And finally, the customer provides the data for the CA certificate to make know who is inspecting and filtering the encrypted data.

Network Composer terminates the SSL connection from the Client and creates a second SSL connection to the Web server. This allows the HTTPS secure web traffic to be inspected

With SSL Full Content Filtering strict checking of the certificate from the server can be performed. The certificate is validated by checking the issuer against a list of trusted CA's and verifying that the certificate is not expired. If the certificate cannot be validated then the network administrator can block this request. This is especially effective against SSL anonymous proxies that use self generated and signed certificates.

Advantages
• Content analysis can be done on the content of the web site
• Virus scanning can be completed
• Spyware MD5 sum matching can be completed
• Spyware Class ID matching can be completed
• Streaming media is properly identified and can be bandwidth-controlled
• File and MIME type extraction and filtering can be completed
• SSL anonymous proxies that are not caught by the database are filtered by content
analysis for categorization and logging

CYMPHONIX

• Reverse DNS lookups are done for IP address URL's
• It is very difficult to circumvent filtering using anonymous proxies
• Moves the SSL security decisions out of the hands of the user and to the network administrator

Disadvantages
• A CA certificate needs to be installed in the browser to prevent an SSL warning
• The not all of the original certificate issuer information is viewable by the user
• High performance cost

SSL Filtering Method Feature Matrix

Cymphonix solution
Both of the above methods are available in Network Composer version 8.0. SSL Full Content Filtering is the recommended method to use to prevent possible circumvention of the filtering.

Feature	SSL Certificate Filtering	SSL Certificate Filtering with Denied Access Page	SSL Full Content Filtering
URL Database Categorization	X	X	X
Spyware URL Database	X	X	X
URL Keyword Search			X
Denied Access Page		X	X
More vulnerable to SSL proxies	X	X	
Virus Scanning			X
Spyware MD5 Sum			X
Spyware Class ID lookup			X
Reverse DNS Lookup			X
Content Analysis			X
File Type Filtering			X
MIME Type Filtering			X
Streaming Media Control			X
View original certificate	XX		
CA Certificate install needed			X
CA Certificate Verification			X

Conclusion
With the increase in Secure Web Traffic (HTTPS) and growing number of 3rd party sites that allow users to bypass current content filtering solutions the ability to have FULL visibility and control over HTTPS traffic is paramount. Any organizations, especially highly-regulated organizations (e.g., education, government, and healthcare) owe it to their users to provide the most robust technology available to ensure ALL web traffic is being filtered and controlled. The Version 8.0 release from Cymphonix provides complete visibility into HTTPS traffic.

References:
1. SSL Traffic Clogs WANS, *PC World*, 03/07/2007, http://www.pcworld.com/article/id,129648/article.html

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

CYMPHONIX