



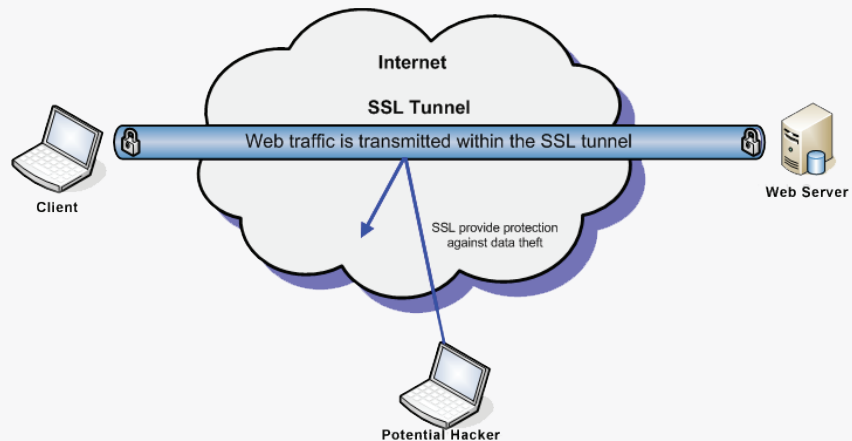
HTTPS/SSL Filtering

Decrypt & Re-encrypting Traffic

The Problem

Web 2.0 applications such as IM, P2P and hosted applications and services are overwhelmingly the majority of the new applications being deployed in networks today. Many of these applications and services are business critical and are hosted in the cloud or offsite by 3rd party companies. This deployment strategy requires many of these services and applications to be accessed over the public Internet using SSL encryption to ensure security. Employees continue to increase the amount of personal business conducted online which adds to growth of SSL traffic. Organizations are doubling the amount of traffic they had a year ago (8 to 11% doubling now to 16 to 22%) and the trend is expected to continue (Source: Cymphonix Labs)

There is a constant, measureable increase in the amount of applications and web services that use Secure Socket Layer (SSL) communications. The encrypted nature of the traffic makes it invisible to many organizations. If it cannot be seen, it cannot be inspected or controlled and therefore comprises a serious threat. In a recent survey of Cymphonix customers nearly 69 percent believe that not having control or visibility over this SSL traffic makes it difficult for the organization to comply with regulations and impossible to enforce Internet usage policies.



Why It Matters

This increase in SSL traffic also increases the amount of blind spots the IT directors face resulting in performance, control and ultimately security issues. Traditional security and content filtering solutions cannot effectively filter and control applications and information outside of the network which makes using the benefits (speed of deployment, cost savings, redundancy, fulfilling "green" initiatives) of these hosted applications and services (like salesforce.com and online storage) difficult. Many organizations know they are blind to their users' SSL traffic, and are searching for a cost effective method to deal with the problem.

Attempts at filtering and controlling SSL traffic using basic identification methods are failing. Many solutions try to accurately detect requests for information by looking at the SSL certificate or assuming that all traffic moving over a specific port is safe. Many times the information in the certificate is provided by a hosting company resulting in confusion and false positives and ultimately an ineffective way of controlling SSL traffic. In addition relying solely on port based control methods has proven

NETWORK COMPOSER FEATURES:

VISIBILITY

- Complete Traffic Visibility™
- Application Traffic (including Layer 7)
- Web 2.0 Content
- Users/Group/Device Activity
- Web, P2P, Anonymous Proxy Traffic
- Malware Threats
- Traffic Trends
- Active Reporting with Multi-Correlation of Data
- Bandwidth Usage Reports

SECURITY

- Complete Traffic Protection™
- Anonymous Proxy Guard™
- Zero-day Threat Protection
- Triple Layer URL / Web 2.0 Filtering
- Malicious Web Site Blocking
- Web 2.0 Infected Site Detection
- Spyware Removal

CONTROL

- Complete Traffic Management™
- Internet Traffic Acceleration/Optimization
- Dynamic Application/Bandwidth Shaping and Allocation
- Web Content Prioritization
- Web Category/URL Shaping
- Web 2.0 management

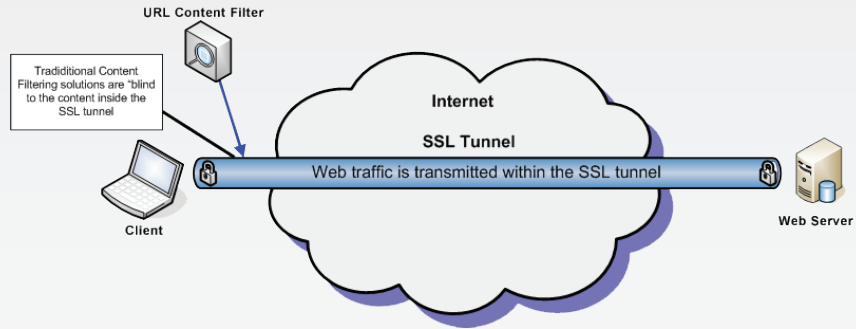
"Money well spent! We look at the reports several times a day and forward any concerns to the principal for discipline."

--Technology Director
Bandera Independent
School District



problematic and cannot provide sufficient security and performance increases.

Figure 2. Traditional Content Filter



SSL is also a free and easy way to bypass existing content filters. Most effective methods employed today use some form of SSL encryption to gain unfiltered access to the Internet. Open access to the Internet via SSL filter avoidance can create major congestion—a simple SSL proxy connection to a media heavy web site like YouTube or Hulu can produce Gigabits of unnecessary bandwidth causing delays and failures of desired traffic.

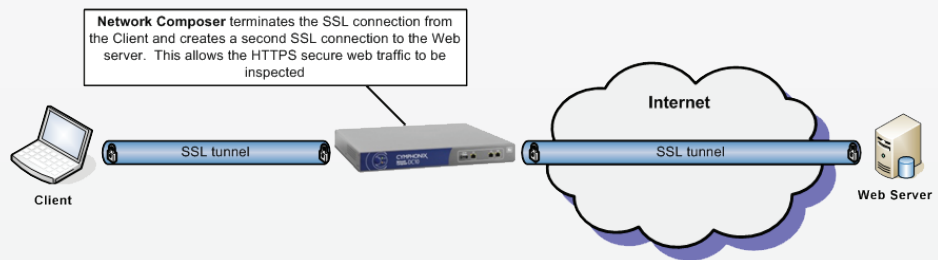
How Cymphonix Solves the Problem

The only way to accurately identify and filter all SSL(HTTPS) traffic is to decrypt the request, apply the desired Internet usage rules then either re-encrypt the request and let it continue or block the request and inform the appropriate client. This method is commonly referred to as Man in the Middle.

Cymphonix Network Composer understands and controls SSL traffic as it leaves the network. In processing this traffic, the Composer ensures that business relevant applications and services are not slowed down or impeded in any way. Cymphonix offers:

- Multiple levels of SSL filtering and control:
 - Certificate inspection
 - Certificate analysis mode
 - Fully terminate and inspect the traffic
- Let known SSL traffic move through un-impeded
- Prioritize known, appropriate traffic
- SSL bandwidth controls
- Application controls
- Detailed reporting
- Shape traffic by site, category, file type or mime type

Figure 3. Network Composer - Full HTTPS Filtering



To find out more about Cymphonix Network Composer and how it can help you control HTTPS/SSL traffic call us at 866-511-1155 or visit us online at www.cymphonix.com.

Reinvent Your Relationship with the Internet.

Network Composer is ready to offer your organization new levels of Internet safety, performance, and control, so you can maximize the value and productivity of your Internet connection. Visit www.cymphonix.com to learn more and schedule a live demo.

Call us at: 866.511.1155

Visit our website at:
www.cymphonix.com

