WAVECREST
COMPUTING

CyBlock SSL Inspection

Introduction to SSL Inspection

General. The SSL Inspection feature is a new value-added, security enhancement incorporated into CyBlock. As explained in more detail later, SSL Inspection will enable CyBlock to analyze encrypted (HTTPS) employee Web traffic. This in turn will help organizations to better identify and defeat security threats. Traffic that "passes inspection" will be promptly forwarded to the Web. *Traffic that does not pass inspection will be blocked.*

Note: When desired, product administrators can specify certain standard and/or custom URL categories to be *exempted* from the inspection process; this is known as "tunneling."

> **Definition of Tunneling.** To understand SSL inspection, we will first discuss the concept of tunneling. In addition to tunneling, you will sometimes see or hear the words "tunneled" and "tunnel" in other communications relating to encryption and inspection of Web traffic. For our purposes, all three of these terms refer to the passage of an SSL-encrypted message through a proxy without being inspected. This is called *tunneling*. A *tunneled* message is one whose URL is exempt from the SSL inspection process. Finally, a *tunnel* is the route that the exempt message takes as it goes through the proxy and bypasses the SSL inspection mechanism.

Benefits to the Organization. SSL inspection leads to more accurate filtering and reporting, which in turn prevents many security threats that hide inside SSL-encrypted data.

SSL Encryption. To understand SSL inspection, it is necessary first to understand a bit about SSL encryption.

> **Positives.** SSL encryption itself is not inherently a problem. Its purpose is basically positive. SSL encryption is being increasingly used to protect the privacy and confidentiality of company and personal data on the Web. Why the increase? In huge numbers, more and more organizations, particularly e-businesses, are using Web-enabled applications that involve the use of personal, private, and/or sensitive data. Banking, online shopping, and credit card transactions are good examples, but by no means the only ones. Surveys show that 25%-35% of enterprise traffic is SSL-encrypted, and the number can be as high as 70% in specific industries. SSL encryption is the most cost-effective way of protecting the privacy of that traffic.
>
> **Negatives.** While SSL encryption solves many privacy-protection problems, it can allow traffic that poses security threats–both inbound and outbound–to pass through security protection measures uninspected and unchecked.
>
> > **Inbound Problem.** SSL encryption creates security blind spots in incoming traffic. The traditional security infrastructure that protects an organization is blind to the threats in inbound SSL traffic and provides an easy vehicle for criminals and hackers to hide their cyber attacks.
> >
> > **Outbound Problem.** In addition to the risks of incoming threats hiding over SSL channels bypassing security protections, outbound enterprise traffic is now a growing problem. This is becoming quite a "hot button" for security applications (e.g., content filtering applications) that tackle data loss prevention (DLP), compliance reporting, and lawful intercept. In the past these solutions could see what was outgoing, but now they are suddenly "in the dark" when it comes to the data transferred over SSL.

Conclusion. Bottom line–SSL encryption undermines security protections. From a security standpoint, most organizations already deploy an array of network and security appliances and programs to protect their enterprise, enforce internal corporate acceptable use policies, and satisfy external government regulation. Unfortunately, in many instances, they can only inspect plaintext traffic and are unable to inspect SSL-encrypted communications for attack signatures. This makes it difficult or impossible for network administrators to enforce corporate acceptable use policies and/or ensure that threats, such as viruses, spam, and malware, are stopped before they reach individual users.

In addition, without the ability to examine the contents of SSL communications, network administrators leave open the possibility for information to be accidentally leaked out of the enterprise or worse, stolen. Regulatory compliance requirements, including identifying accidental or intentional leakage of confidential information, are also virtually impossible to meet because of SSL encryption.

The CyBlock SSL Inspection Solution

What is SSL Inspection? SSL inspection is a CyBlock process that analyzes employees' encrypted Web requests (HTTPS traffic). Its goal is to determine the specific type of content that the employee is seeking. This enables CyBlock to properly categorize the traffic based on the most specific level of content-identification elements in the requested URL. This includes the path and parameters–not just the domain name. The total SSL inspection process decrypts, analyzes, categorizes, and then re-encrypts the traffic. If the categorization phase does not result in the request being blocked, CyBlock then passes the request on to the Web.

How Does SSL Inspection Improve Categorization? First, let us see what happens when SSL-encrypted traffic is not inspected (i.e., tunneled). We'll then see what happens when it is inspected.

1. **Traffic Not Inspected.** In dealing with tunneled traffic, CyBlock can identify and categorize the domain, but it:
   - Cannot identify a path included in a URL.
   - Cannot identify or use embedded URLs or parameters for categorization matching, for example, in blocking keywords if logged on to a Google account.
   - Cannot inspect content for malware.

2. **Traffic Inspected.** In addition to identifying the domain, CyBlock will be able to:
   - Identify the path included in the URL.
   - Identify and use paths, embedded URLs, or parameters (for matching)–and thus perform more granular categorization.
   - Inspect content for malware.

Note: Be aware that SSL inspection may entail a certain amount of latency (delay) as the traffic is decrypted, inspected, and re-encrypted. Consequently, it should only be used where necessary–as decided by the organization. In fact, we believe that–as much as possible–many companies will exempt traffic to trusted, mission-critical destinations.

SSL Inspection Setup. Because inspection of encrypted traffic is desirable but not without consequences, we assume that companies will want to use it selectively. That is why our SSL Inspection feature includes the ability for product administrators to configure SSL inspection that is optimum for their own organization. The structure has the following two dimensions: Groups and IDs, and standard and custom categories. The setup logic goes like this:

1. For inspection to occur, you select at least one group or ID for inspection.
2. By default, all traffic to all categories, except the Financial category, is set to be inspected.
3. You can select certain categories to be exempted from inspection; this is called tunneling.
4. Traffic from employees selected in Step 1 to categories that have not been exempted in Step 3 will be inspected.

Setup and Implementation

General. The product administrator uses the **Advanced Settings - Proxy Settings - SSL Inspection** screen to configure SSL inspection. Before discussing using this screen though, let us take a look at some more general issues.

Three Modes of SSL Inspection. Before working with the screen, we recommend that you decide on one of the three modes of SSL inspection:

1. **Zero Inspection Mode.** Under this approach, all traffic is passed through the CyBlock product without being subjected to SSL inspection. This may be risky from a security standpoint, but it avoids performance/speed issues. Under this choice, all traffic will be tunneled.

   Action: No action required during initial setup.

2. **Blanket Mode.** This approach mandates that all encrypted traffic be inspected regardless of source or destination. (**Note:** Depending on traffic volume, this choice could cause performance problems.)

   Action: The product administrator selects “Enterprise” in the appropriate box in the setup screen. No other action is required.

3. **Selective Inspection Mode.** This approach is more flexible than the two above. It can be expressed as follows: “Inspection will apply only to encrypted traffic that originates with selected users AND is bound for categories that have not been tunneled.” As a corollary, traffic from undesignated users to tunneled categories will not be inspected.

   Action: In general, the product administrator:
   - Selects the specific groups and/or users whose visit requests are to be inspected.
   - Selects the specific categories to be exempt from inspection, if any.

Because it is the most involved of the three modes, the Selective Inspection Mode is discussed in more detail a bit later.

Note: Whether visit requests are inspected or not, they are all categorized. In most cases, SSL inspection is simply a pre-categorization step for certain URLs.

The three modes are illustrated in the following diagram.

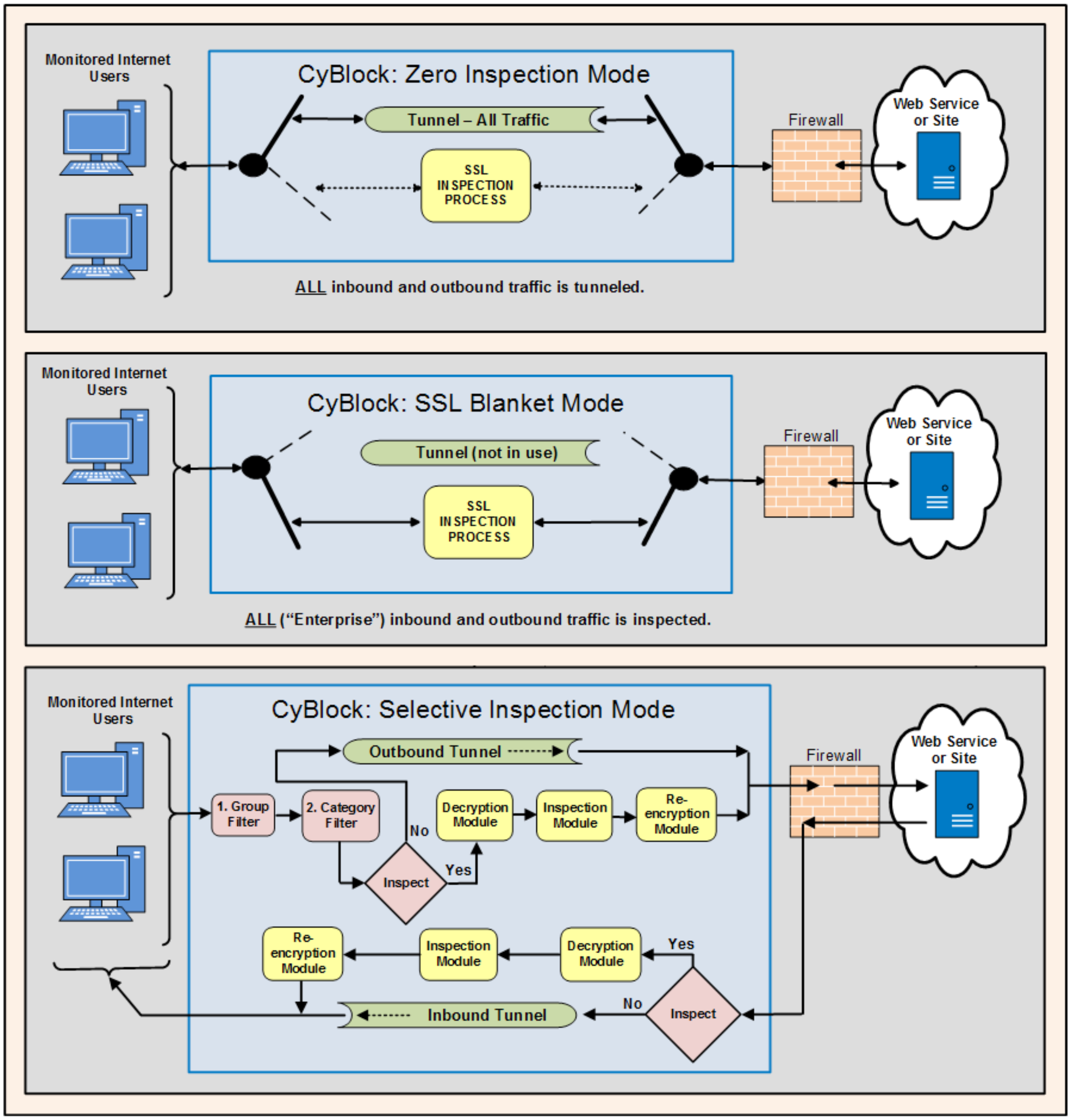


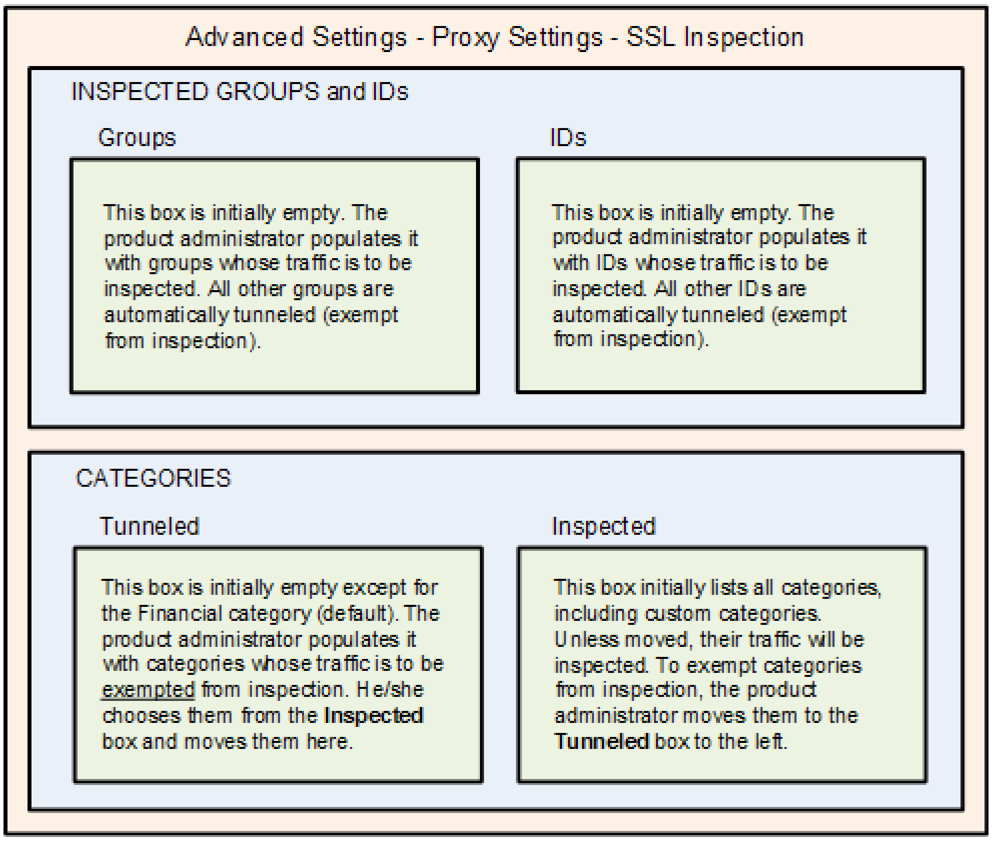
Figure 1 - Three Modes of SSL Inspection

Using Custom Categories. As with other policy setups (filtering, bandwidth management, etc.), custom categories can be very useful in implementing a fine-tuned, precisely targeted SSL inspection routine. For example, a custom category can be created to ensure that some of the encrypted URLs in a particular category are inspected. In this case, the product administrator creates a custom category and enters the "target" URLs. The product administrator can create another custom category to ensure inspection of local-interest URLs that are not in our URL List. Another can be created to exempt from inspection some of the encrypted URLs in a particular category.

SSL Inspection Setup Screen. Illustrated in the following figure, the screen has two major sections:

- **Inspected Groups and IDs.** This section is used to choose groups and/or individual users (IDs) whose traffic is to be inspected.

- **Categories.** This section is used to choose standard and/or custom categories that are to be tunneled (i.e., exempted from inspection). Traffic to categories that are not tunneled AND that originates with the designated users will be inspected.



Advanced Settings - Proxy Settings - SSL Inspection

INSPECTED GROUPS and IDs

Groups

This box is initially empty. The product administrator populates it with groups whose traffic is to be inspected. All other groups are automatically tunneled (exempt from inspection).

IDs

This box is initially empty. The product administrator populates it with IDs whose traffic is to be inspected. All other IDs are automatically tunneled (exempt from inspection).

CATEGORIES

Tunneled

This box is initially empty except for the Financial category (default). The product administrator populates it with categories whose traffic is to be exempted from inspection. He/she chooses them from the **Inspected** box and moves them here.

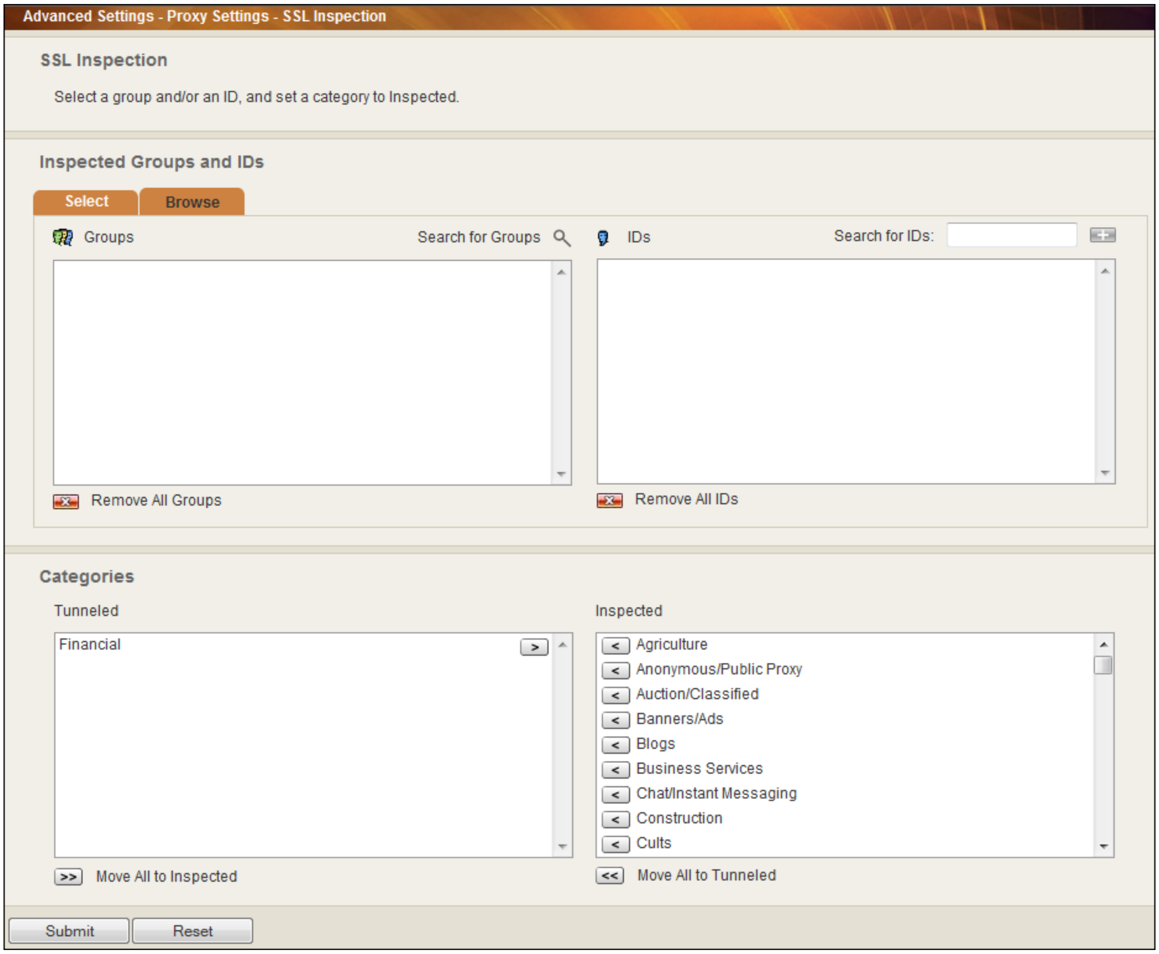
Inspected

This box initially lists all categories, including custom categories. Unless moved, their traffic will be inspected. To exempt categories from inspection, the product administrator moves them to the **Tunneled** box to the left.

Figure 2 - SSL Inspection Setup Screen Concept

Note: The screen has default settings that prevent any inspection from taking place. In addition, the Financial category will not be inspected and will appear in the Tunneled box. This is a recommended setting which you can easily change.

The following figure shows the setup screen.


Advanced Settings - Proxy Settings - SSL Inspection

SSL Inspection

Select a group and/or an ID, and set a category to Inspected.

Inspected Groups and IDs

Categories

Tunneled: Financial

Inspected: Agriculture, Anonymous/Public Proxy, Auction/Classified, Banners/Ads, Blogs, Business Services, Chat/Instant Messaging, Construction, Cults

Figure 3 - SSL Inspection Setup Screen

Rationale for the Selective Inspection Mode. Although the Selective Inspection Mode is the most involved, many companies will want to implement it. The reason is that a certain number of your employees may need to work regularly with a select set of mission-critical Web applications and Web sites (URLs). If these are considered trustworthy and safe from a security perspective, management will not want to interfere with or slow down the related traffic by insisting that traffic from them be inspected. On the other hand, management will want to protect the company from as many security threats as possible and will want all other encrypted traffic inspected.

Setting Up the Selective Inspection Mode. Companies will vary in their use of this approach, but in general they will follow these steps:

1. Determine the groups, IDs, and standard categories to be included in the inspection process.
2. Determine the standard categories to be excluded (tunneled) from the inspection process.
3. Decide on the use of custom categories and create them if desired. Custom categories will be displayed automatically in the Inspected box of the setup screen.
4. Using the designated boxes in the upper half of the setup screen, select the groups and IDs to be included in the inspection process. (Those not selected will automatically be excluded.)
5. In the lower half of the setup screen, move the exempt categories from the Inspected box to the Tunneled box.

Reporting Capabilities. As mentioned previously, SSL inspection leads to more accurate reporting. Full URLs with SSL traffic will be reported in the Real-Time Web Monitor and in audit reports. These audit reports include:

- Category Audit Detail
- Category Audit Summary
- Site Audit Detail
- User Audit Detail
- User Audit Summary

With this full URL information, each report will serve as a more comprehensive auditing tool for management.

Source: Examining SSL-Encrypted Communications - Netronome

About Wavecrest Computing

Wavecrest Computing has provided business and government clients with reliable, accurate Web-use management products since 1996. IT specialists, HR professionals, and business managers trust Wavecrest's Cyfin® and CyBlock® products to manage employee Internet usage – reducing liability risks, improving productivity, saving bandwidth, and controlling costs.

Wavecrest has over 3,000 clients worldwide, including Edward Jones, General Electric, IBM, MillerCoors, New York City Dept. of Transportation, Rolex, Siemens, and a growing list of global enterprises and government agencies. For more information on our company, products, and partners, visit www.wavecrest.net.

WAVECREST
COMPUTING

Wavecrest Computing
2006 Vernon Place
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351
fax: 321-953-5350