Websense Content Gateway: Tunneled Protocol Detection

Tunneled protocol detection analyzes traffic to discover protocols that are tunneled over HTTP and HTTPS. Traffic that is allowed to tunnel over specific ports is also scanned. Such traffic is reported to Websense Web filtering for protocol policy enforcement. When tunneled protocol detection is enabled, scanning is performed on both inbound and outbound traffic, regardless of other scanning settings.

HTTP tunneling occurs when applications that use custom protocols for communication are wrapped in HTTP (meaning that standard HTTP request/response formatting is present) in order to use the ports designated for HTTP/HTTPS traffic. These ports are open to allow traffic to and from the Web. HTTP tunneling allows these applications to bypass firewalls and proxies, leaving a system vulnerable.

The tunneled protocol detection feature scans HTTP and HTTPS traffic and, when it detects a protocol, forwards it to Websense Web filtering for policy enforcement. At this point, a protocol is blocked or allowed based on policy definitions. This feature can be used to block protocols used for instant messaging, peer-to-peer applications, and proxy avoidance.

This paper includes the following topics:

Google Wave and Gmail Chat protocol signatures

Paper 70000 / Updated: 18-May-2010

Applies to:	Websense Web Security Gateway v7.5.x Websense Web Security Gateway Anywhere v7.5.x Websense Content Gateway v7.5.x

Websense Web Security Gateway now includes signatures to allow Websense Web Security Gateway and Web Security Gateway Anywhere to filter the Google Wave and Gmail Chat protocols on HTTPS.

Google Wave allows users to collaborate in real time via conversation and shared files, including documents, videos, and photos. Gmail Chat is a Google Talk feature that lets users send and receive instant messages.

Google Wave appears in the Web Security Manager Protocols window in the P2P File Sharing category. Gmail Chat is listed in the Instant Messaging / Chat category. Labeled "(WSG only)" in the Protocols window, these signatures are filtered only if Secure Sockets Layer (SSL) decryption and the tunneled protocol detection feature are enabled in the Web Security Manager Settings tab Scanning Options. See TRITON – Web Security Help for information about the tunneled protocol detection feature.

Important

You should note that as of version 7.5, Network Agent no longer detects and filters the Gmail Chat protocol in Websense Web Filter and Websense Web Security.

Google announced in January 2010 that all Gmail traffic would be encrypted, to protect users in Wi-Fi environments. Because Network Agent cannot detect encrypted traffic, it cannot filter the Gmail Chat protocol.

No workaround for this issue exists for current Websense Web Security/Websense Web Filter users. You must upgrade to Websense Web Security Gateway version 7.5 to filter Gmail Chat.

Related topics:

HTTPS tunneled protocol connection dropped by Websense Content Gateway

Websense Content Gateway connection dropped for non-standard HTTPS

Tunneled protocols not detected by Websense Content Gateway

HTTPS tunneled protocol connection dropped by Websense Content Gateway

Paper 70001 / Updated: 18-May-2010

Applies to:	Websense Web Security Gateway v7.5.x Websense Web Security Gateway Anywhere v7.5.x Websense Content Gateway v7.5.x

Overview

A protocol tunneled on HTTPS may not be able to establish a connection with Websense Content Gateway. America Online, Skype, and Tencent QQ are examples of application protocols that may not be able to connect with the proxy.

One reason a tunneled protocol connection may be dropped is if the application does not trust the Websense certificate that has been imported into the Trusted Root Certification Authorities. America Online is an example of a protocol connection that can be dropped in this particular situation.

Possible resolutions to this issue may include:

- Importing a proxy certificate for computer account
- Disabling the proxy's HTTPS option
- Using the proxy's SSL category bypass feature

Importing a proxy certificate for computer account

For applications like America Online that do not trust the Websense certificate, you may resolve this situation by importing a proxy certificate for the computer account. Note that importing the certificate via a browser imports the certificate only for the current user, not the computer.

Use the following procedure to import a proxy certificate for a computer account:

1. In the Windows Command Prompt, enter **mmc.exe**. The Console dialog box appears.
2. In the Add/Remove Snap-in dialog box, click **Add**.
3. In the Add Standalone Snap-in dialog box, double-click **Certificates**. The Certificates snap-in wizard appears.
4. Select **Computer account** and click **Next**.
5. Indicate that you want the snap-in to always manage **Local computer**. Click **Finish**.
6. **Close** the Add Standalone Snap-in dialog box and click **OK** in the Add/Remove Snap-in dialog box.
7. Expand the Console Root tree in the left pane of the Console dialog box. Navigate to **Trusted Root Certification Authorities > Certificates**.
8. Right-click **Certificates** and select **All Tasks > Import** to open the Certificate Import Wizard. Click **Next**.
9. Browse to the proxy's Public Root Certificate Key file exported from the SSL Manager and import it. Confirm that the certificate appears in the Trusted Certificate Authorities Certificate Store.
10. Close the Console dialog box. You do not need to save settings.

Disabling the proxy's HTTPS option

You can also disable the HTTPS option in Websense Content Gateway to allow a tunneled protocol connection. However, if you choose this alternative, you lose valuable Content Gateway features. See Websense Content Gateway Online Help for information about SSL Manager features.

Using the proxy's SSL category bypass feature

Application protocols like America Online, Skype, and Tencent QQ fall into either the Instant Messaging or Uncategorized Websense Web site category. You can use the SSL category bypass settings in the Websense Web Security Manager to allow these protocols to bypass proxy inspection and establish a network connection.

On the Web Security Manager **Settings** tab:

1. Select **SSL Decryption Bypass**.
2. Click the **Instant Messaging** or **Uncategorized** category check box, depending on the protocol you wish to bypass.
3. Click the arrow to the right of the category tree to enter the selected category into the **Categories selected for SSL decryption bypass** box.

You should use this solution with care, because when you specify a category for bypass, all application protocols identified in that category are allowed to bypass the proxy.

If you want to allow only a particular application protocol to bypass the proxy, you can specify the individual hostname or IP address for the protocol in the hostname or IP address bypass list in the SSL Decryption Bypass page. However, you should note that some IP addresses can change dynamically, making this implementation somewhat impractical. See TRITON – Web Security Help for information about the SSL category bypass feature.

Related topics:

Google Wave and Gmail Chat protocol signatures

Websense Content Gateway connection dropped for non-standard HTTPS

Tunneled protocols not detected by Websense Content Gateway

Websense Content Gateway connection dropped for non-standard HTTPS

Paper 70002 / Updated: 05-May-2010

Applies to:	Websense Web Security Gateway v7.5.x Websense Web Security Gateway Anywhere v7.5.x Websense Content Gateway v7.5.x

Overview

Some application protocols that tunnel over port 443 may attempt to establish a connection with Websense Content Gateway using an HTTPS standard that Content Gateway does not recognize. When SSL is enabled, these application protocols cannot connect with Content Gateway. QIP 2005 is an example of this type of application protocol.

When SSL is disabled, this issue does not occur.

You may resolve this issue in one of two ways:

- Configuring the Content Gateway to tunnel all unknown protocols
- Adding incidents to the Content Gateway SSL incidents list to tunnel these application protocols

Tunneling unknown protocols

You can configure Websense Content Gateway to tunnel all unknown protocols. This option can provide a consistent workaround for establishing a connection regardless of the number of destination origin servers or dynamic IP address changes. However, you should be aware that because this option allows all traffic to tunnel through port 443, you may be opening your network to malicious traffic.

Use the following procedure to accomplish this task:

1. Run **export LD_LIBRARY_PATH=/opt/WCG/sxsuite/lib**.
2. Run **/opt/WCG/sxsuite/bin/oemtool profileconfig 1 tunnel_unknown_protocols yes**.
3. Run **/opt/WCG/sxsuite/bin/oemtool get profileconfig 1 tunnel_unknown_protocols** to confirm the parameter change.
4. Restart Websense Content Gateway.

Adding SSL incidents

You can add a URL to the SSL Manager incident list to allow Content Gateway to tunnel individual HTTPS Web site client requests. This option has the advantage of

easy configuration in the Content Gateway Manager interface. However, it may be a highly impractical alternative if a large number of IP addresses must be entered, or if any of those IP addresses change dynamically.

Use the following procedure to accomplish this task:

1. In the Content Gateway Manager, navigate to the **Add Website** page and specify a site request that you want to tunnel (**Configure > SSL > Incidents**).
2. Select **By URL**.
3. In the Action drop-down list, select **Tunnel**.
4. Click **Add URL**.

Related topics:

Google Wave and Gmail Chat protocol signatures

HTTPS tunneled protocol connection dropped by Websense Content Gateway

Tunneled protocols not detected by Websense Content Gateway

Tunneled protocols not detected by Websense Content Gateway

Paper 70003 / Updated: 05-May-2010

Applies to:	Websense Web Security Gateway v7.5.x Websense Web Security Gateway Anywhere v7.5.x Websense Content Gateway v7.5.x

Overview

The Websense Content Gateway tunneled protocol detection feature scans HTTP and HTTPS traffic and, when it detects a protocol, forwards it to Websense Web filtering for policy enforcement. At this point, a protocol is blocked or allowed based on policy definitions.

If application protocols are not detected by this feature, policies to control specific protocol traffic may not be enforced.

This situation may occur in one of the following instances:

- When an application uses a non-HTTP/HTTPS port. Microsoft Network (MSN) Messenger and Yahoo! Messenger are examples of such an application.

  Attachments transferred via the Yahoo! Messenger application protocol also use a non-HTTP/HTTPS port and may not be detected.
- If an application protocol that uses an HTTP/HTTPS port can switch to a non-HTTP/HTTPS port after it is detected and blocked on its first connection

attempt. For example, applications like Skype and Google Talk can change the port they use dynamically, avoid the proxy's tunneled protocol detection, and connect directly to an outside server.

© When an application protocol tunnels over HTTPS, and the HTTPS feature is disabled in the Content Gateway. America Online (AOL) and Google Talk are examples of protocols that tunnel over HTTPS.

Network Agent

In the first two cases, the tunneled protocols not caught by the Content Gateway can be detected by the Websense Network Agent component, which can be configured to monitor all non-HTTP/HTTPS ports when the protocol management feature is enabled. See Network Agent configuration in the TRITON – Web Security Help for more information.

In the third case, when an application protocol tunnels over HTTPS and the Content Gateway HTTPS feature is disabled, Network Agent may detect it based on the host address.

If Network Agent is not deployed to monitor ports that bypass the Content Gateway, you can configure the firewall to block those ports, forcing the client traffic through the proxy. Note that this type of firewall blocking may result in some applications not working properly.

HTTPS option

You must enable the HTTPS feature in the Content Gateway Manager interface in order to detect protocols that tunnel over HTTPS:

1. Navigate to the **General** tab (**Configure > My Proxy > Basic**).
2. In the Features section, select **HTTPS**.
3. Click **Apply**.
4. Click **Restart**.

Related topics:

Google Wave and Gmail Chat protocol signatures

HTTPS tunneled protocol connection dropped by Websense Content Gateway

Websense Content Gateway connection dropped for non-standard HTTPS