Content Gateway v7.5: Troubleshooting

Topic 60000 / Updated: 16-June-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

Installing the ARM on Red Hat Enterprise Linux 5, update 5

Dropped HTTPS connections

Sites that have difficulty transiting Content Gateway

- *Citrix collaboration products*
- *WebEx*
- *Firefox Update*
- *Pandora.com*
- *Real Networks Real Player*

Sites that host applications that don't handle NTLM authentication

Restricted users fail to authenticate with NTLM

Installing the ARM on Red Hat Enterprise Linux 5, update 5

Topic 60022 / Updated: 12-July-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

When installing Content Gateway on Red Hat Enterprise Linux 5, update 5 (base or Advanced Platform; 32-bit only), the installer displays a warning that the kernel version is not supported. When 'y' is selected to continue the installation, the installation appears to complete normally. However, the Release Notes state that the

ARM was not installed. How is the ARM installed on Red Hat Enterprise Linux 5, update 5?

To install the ARM on Red Hat Enterprise Linux 5, update 5:

- The **arm_install.sh** file must be updated
- The installation tar file must be rebuilt
- Content Gateway must be reinstalled.

Perform the following steps to complete the process:

1. Log in and become root on the Content Gateway host system.
2. Change directory to the unpacked Content Gateway installation directory. Files in this directory include:

   adm_help.tar

   dss.tar

   lx86_arms_2.6.18-128.tar

   lx86_arms_2.6.18-164.tar

   lx86_arms_2.6.18-53.tar

   lx86_arms_2.6.18-8.tar

   lx86_arms_2.6.18-92.tar

   lx86_arms_2.6.9-55.tar

   lx86_arms_2.6.9-67.tar

   lx86_arms_2.6.9-78.tar

   lx86_arms_2.6.9-89.tar

   lx86inst.tar

   lx86.tar

   mds.tar

   plugins.tar

   subscription.txt

   wcg_config.sh

   wcg_install.sh

   wcg.tar

   wcg_uninstall.sh

   WSGAsubscription.txt
3. Unpack **lx86inst.tar**.

   tar -xvf lx86inst.tar
4. Remove **lx86inst.tar**.

   rm -f lx86inst.tar
5. Edit **arm_install.sh**.

   vi scripts/arm_install.sh
6. Replace line 205: armtar="none"

with the following lines:

```
echo "Installing for 2.6.18-194 kernel" >> $LogFile
armtar="lx86_arms_2.6.18-164.tar"
armdir_smp="linux_x86_2-6-18__rh54_smp"
armdir="$armdir_smp"
```

7. Save the file and exit the editor.
8. Create a new tar file:

   ```
   tar -cf lx86inst.tar scripts bin
   ```

9. Remove the directories left behind from unpacking lx86inst.tar.

   ```
   rm -Rf scripts
   rm -Rf bin
   ```

10. Install Content Gateway.

    ```
    ./wcg_install.sh
    ```

> **Note**
> During installation, the installer will still display a warning that the kernel version is not supported, however, after 'y' is entered to continue the installation, the process completes normally and the ARM is present.

Dropped HTTPS connections

Topic 60009 / Updated: 3-June-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

Some application protocols that tunnel over port 443 may attempt to establish a connection with 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 is not an issue.

The issue is easily resolved in either of two ways:

- Configure Content Gateway to tunnel all unknown protocols.
- Add incidents to the Content Gateway SSL incidents list to tunnel these application protocols.

Tunneling unknown protocols

Content Gateway can be configured to tunnel all unknown protocols. This option provides a consistent workaround for establishing a connection regardless of the

number of destination origin servers or dynamic IP address changes. However, because this option allows all traffic to tunnel through port 443, you may be opening your network to malicious traffic.

To tunnel all unknown protocols, on the Content Gateway host:

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 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. 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.

To add a Web site to the SSL Incident List:

1. In Content Gateway Manager, go to the **Configure > SSL > Incidents > Add Website** tab.
2. In the **URL field** specify the URL that you want to tunnel.
3. Select **By url** and for **Action** select **Tunnel**.
4. Click **Apply**.

Sites that have difficulty transiting Content Gateway

Topic 60001 / Updated: 2-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

Some Web sites host applications and services that have difficulty transiting Websense Content Gateway (and most Web proxies). These sites can present different problems and require different solutions depending on the Web application and the Content Gateway deployment.

Citrix collaboration products

WebEx

Firefox Update

Pandora.com

Real Networks Real Player

Citrix collaboration products

Topic 60002 / Updated: 2-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

Citrix collaboration products do not support HTTPS connections through a proxy. Connections to Citrix collaboration products require proxy bypass rules.

To create proxy bypass rules, you will need a list of current Citrix URL ranges. Go to http://www.citrixonline.com/iprange.

Depending on your Content Gateway configuration, here are 3 options for creating bypass rules for Citrix:

Option 1: Add the Citrix collaboration product URLs to the Content Gateway ARM static bypass list.

1. In Content Gateway Manager, go to **Configure > Networking > ARM > Static Bypass** tab and click **Edit File**.
2. Click **Add** to add the Citrix URLs to the bypass list.
   a. In the **Rule Type** drop-down box select **bypass**.
   b. Leave the **Source IP** field empty.
   c. In the **Destination IP** field, add the range or CIDR of one of the Citrix ranges.
   d. Click **Add**.
3. Repeat steps 'a' through 'd' for each range.
4. When all of the ranges have been added, click **Apply**.

Option 2: If Content Gateway is a transparent proxy with WCCP devices:

Add the Citrix IP address ranges to the WCCP access control list.

Option 3: If Content Gateway is an explicit proxy that uses a PAC file:

Add entries for the Citrix URLs in the exceptions block of your PAC file. A separate line is required for each distinct IP address range.

```
if (shExpMatch(url, "Citrix Collaboration IP address"))
{return "DIRECT";}
```

where "Citrix Collaboration IP address" is replaced by an IP address range from the Citrix list.

Related topics:

WebEx

Firefox Update

Pandora.com

Real Networks Real Player

WebEx

Topic 60003 / Updated: 2-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

WebEx does not support HTTPS connections through a proxy. However, there are several easy workarounds.

Option 1: Add the WebEx URL to the SSL Incident list as Action=Tunnel.

1. In Content Manager, go to the **Configure > SSL > Incidents > Add Website** tab.
2. In the **URL field** add: *.webex.com
3. Select **By url** and for **Action** choose **Tunnel**.
4. Click **Apply**.

Option 2: If Content Gateway is an explicit proxy that uses a PAC file:

Add an entry for WebEx in the exceptions block of your PAC file:

```
if (shExpMatch(url, "*.webex.com/*")) {return "DIRECT";}
```

Option 3: If Content Gateway is an explicit proxy that does not use a PAC file:

On each client, add an exception to the proxy settings list.

The following steps are for Microsoft Windows systems only. For other systems, consult your operating system and browser documentation.

On Windows systems, the following configuration works for all browsers because the WebEx client uses the values stored in **Internet Options > LAN Settings > Proxy Settings**.

1. Open the Windows **Control Panel** and select **Internet Options**.
2. Select the **Connection** tab and click **LAN Settings**.
3. In the **Proxy server** area, click **Advanced**.
4. In the **Exceptions** entry field add: ***.webex.com**
5. Click **OK**; repeat until **Internet Options** is closed.
6. Close and reopen any open browsers.

If the connection still fails

In some cases, the WebEx site responds with an IP address or a domain name that doesn't match *.webex.com.

You can work around the problem by examining the **inbound_access.log** to find the unresolved connection and then add the IP address or domain name as an exception using the option employed above.

1. On the Content Gateway host, change directory to **/opt/WCG/sxsuite/log** and open or view **inbound_access.log** (/opt/WCG is the default installation path; substitute your installation path).
2. Most often, the unresolved CONNECT will be in close proximity to a successful *.webex.com connect, so start by searching for webex.com. A successful tunnel connection looks similar to:

   CONNECT cisco.webex.com:443 HTTP/1.0
   CONNECT nsj1msccl01.webex.com:443 HTTP/1.1
   (tunneled SSL connection to nsj1msccl01.webex.com:443)
   (tunneled SSL connection to cisco.webex.com:443)
3. From this location scan downward for a URL that has the CONNECT status, but does not indicate that the connect was tunneled or successfully fetched content with a GET. This unresolved traffic might look similar to:

   CONNECT 66.114.169.162:443 HTTP/1.1
   CONNECT 66.114.169.162:443 HTTP/1.1
4. Add the domain name or IP address to the incident list or bypass list.

WebEx domain, IP addresses, and ports (15-July-2009):

World Wide URL domain exception = *.webex.com

USA IP addresses:

USA IP exception = 64.68.96.0 to 64.68.127.255 and 66.114.160.0 to 66.114.175.255
USA CIDR exception = 64.68.96.0/19 and 66.114.160.0/20

Outside the USA IP addresses:

IP Exception = 62.109.200.0 - 62.109.201.255 and 210.4.200.0 to 210.4.201.255
CIDR exception = 62.109.201.0/23 and 210.4.201.0/23

Ports that need to open to clients (Internet):

TCP 80 Client Access

TCP 443 Client Access

TCP 8554 Audio Streaming Client Access

UDP 7500 Audio Streaming

UDP 7501 Audio Streaming

UDP 9000 VOIP/Video

UDP 9001 VOIP/Video

Related topics:

Citrix collaboration products

Firefox Update

Pandora.com

Real Networks Real Player

Firefox Update

Topic 60004 / Updated: 2-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

Firefox Update does not support HTTPS connections through a proxy.

To work around the problem, add the URL of the Firefox Update site to the SSL Incident list as Action=Tunnel.

1. In Content Manager, go to the **Configure > SSL > Incidents > Add Website** tab.
2. In the **URL field** add: https://aus2.mozilla.org
3. Select **By url** and for **Action** choose **Tunnel**.
4. Click **Apply**.

Related topics:

Citrix collaboration products

WebEx

Pandora.com

Real Networks Real Player

Pandora.com

Topic 60005 / Updated: 2-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

Pandora.com does not support HTTPS connections through a proxy.

To work around the problem, add Pandora.com to the SSL Incident list as Action=Tunnel.

1. In Content Manager, go to the **Configure > SSL > Incidents > Add Website** tab.
2. In the **URL field** add: https://pandora.com
3. Select **By url** and for **Action** choose **Tunnel**.
4. Click **Apply**.

Related topics:

Citrix collaboration products

WebEx

Firefox Update

Real Networks Real Player

Real Networks Real Player

Topic 60006 / Updated: 2-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

Real Networks Real Player fails to stream content when the following combined conditions exist:

1. Content Gateway is deployed as an explicit proxy.
2. Content Gateway is the only path to the Internet.
3. NTLM user authentication is configured.

This is because, by default Real Player uses the RTSP or PNA protocols to stream media, both of which bypass Content Gateway. However, when Content Gateway is the only path to the Internet, Real Player uses HTTP to transit Content Gateway. Unfortunately, Real Player doesn't handle NTLM authentication properly and the connection fails.

For related information, see Microsoft knowledge base article http://support.microsoft.com/kb/288734.

To work around the problem in versions 7.5.x and 7.1.4 and later, add an **Allow rule** to **filter.config** that identifies the Real Player application and allows Real Player traffic to bypass Content Gateway:

1. In Content Gateway Manager, go to **Configure > Security > Access Control > Filtering** and click **Edit File**.

2. Add the following filtering rule:

   Rule Type = Allow

   Primary Destination Type = dest_domain

   Primary Destination Value = .

   User-Agent = realplayer

3. Click **Add**. The new rule appears in the table at the top of the page. It should have the format:

   Rule Type=Allow , dest_domain=. , User-Agent=realplayer

4. Click **Apply** and then **Close**.

To work around the problem in versions 7.1.3 and earlier, add an Allow rule to filter.config for each destination that hosts Real Player content you want to allow.

1. In Content Gateway Manager (Websense Content Manager), go to **Configure > Security > Access Control > Filtering** and click **Edit File**.
2. For each destination hosting Real Player content that you want to allow, add a filtering rule:

   Rule Type = Allow

   Primary Destination Type = dest_domain

   Primary Destination Value = URL_of_site

3. Click **Add**. The new rule appears in the table at the top of the page. It should have the format:

   Rule Type=Allow , dest_domain=URL_of_site

4. Click **Apply** and then **Close**.

Related topics:

Citrix collaboration products

WebEx

Firefox Update

Pandora.com

Sites that host applications that don't handle NTLM authentication

Topic 60007 / Updated: 2-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

When Content Gateway is configured to perform NTLM authentication, some Web sites still challenge for credentials. This happens when the Web site hosts an application that is trying to start, but which fails to complete NTLM authentication. This is usually because the application is attempting some non-standard NTLM communication.

If manual authentication is unacceptable, you can create an **allow rule** in **filter.config** for each site that hosts an application that doesn't know how to authenticate. This rule allows the application to bypass authentication.

For example:

1. In Content Manager, go to **Configure > Security > Access Control > Filtering**.
2. Click **Edit File**.
3. Add a rule: Rule Type=allow, dest_domain=example.net
4. Click **Apply** and **Close**.
5. On the Linux command line, in **/opt/WCG/bin** (substitute your Content Gateway installation location), run:

   ```
   content_line -x
   ```

For more information, see the sections titled **Controlling access to Web sites** and **filter.config** in the Websense Content Manager online Help.

Restricted users fail to authenticate with NTLM

Topic 60012 / Updated: 3-June-2010

Applies To:	Websense Content Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway 7.5, 7.1, 7.0 Websense Web Security Gateway Anywhere 7.5

When Content Gateway is configured to perform NTLM authentication with Active Directory, users who are restricted to a subset of workstations may not successfully authenticate.

The problem is due to the way Content Gateway establishes a session with the domain controller.

To work around the problem, in your Active Directory add a workstation named "TMP" and include it in the set of workstations available to the restricted users.

NOTE: TMP is the surrogate workstation name used by Content Gateway when establishing a session. TMP is used because, for security reasons, the actual workstation name is not provided by the browser in the authentication handshake.