Content Gateway v7.5: Frequently Asked Questions

Topic 60008 / Updated: 3-June-2010

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

How do I configure IPTables to harden the Content Gateway host system?

Topic 60010 / Updated: 3-June-2010

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

When Content Gateway is deployed on a stand-alone server, it is strongly recommended that an IPTables firewall be configured to provide maximum security and efficiency with Content Gateway.

CAUTION: Only qualified system administrators should modify the IPTables firewall.

As an aid to understanding the IPTables configuration required for Content Gateway, a sample IPTables configuration script is installed in the Content Gateway bin directory (/opt/WCG/bin, by default). The sample script is named **example_iptables.sh**.

- Review the script carefully.
- Do not use the script directly.
- Create your own script that meets your specific needs.

To view a text file version of the sample script, click here. Note: The sample script available here may not be the latest version. The sample script installed in the Content Gateway bin directory is the most up-to-date version.

Configuration:

The following list of rules is organized into groups that address different deployments. Be sure the **/etc/sysconfig/iptables** file contains all the rules that apply to your network from each section.

If the proxy is configured to use multiple NICs, for each rule that applies to an interface, specify the appropriate NIC with the "-i" option ("-i" means only match if the incoming packet is on the specified interface). Typically, multiple interfaces are divided into these roles:

- **Management interface** (MGMT_NIC) - The physical interface used by the system administrator to manage the computer.
- **Internet-facing interface** (WAN_NIC) - The physical interface used to request pages from the Internet (usually the most secure interface).
- **Client-facing interface** (CLIENT_NIC) - The physical interface used by the clients to request data from the proxy.
- **Cluster interface** (CLUSTER_NIC) - The physical interface used by the proxy to communicate with members of the cluster.

NOTE: If you customized any ports that Websense software uses for communication, replace the default port shown in the following rules with the custom port you implemented.

All deployments

These rules are required to enable Content Gateway communications, regardless of the deployment.

The following rules should be first.

```
iptables --I OUTPUT -o log -t raw -j NOTRACK
iptables --policy INPUT DROP
```

NOTE: In addition to the above rules, it is a best practice to increase the size of **ip_conntrack_max** to 100000 to improve performance. Typically, this can be done using the following command: **/sbin/sysctl net.ipv4.ip_conntrack_max=100000**. Note that this should be done after iptables is invoked. Also, this change in value will not be preserved after reboot unless you configure your system to set this value upon startup. To do so, add the following line to **/etc/sysctl.conf**: **net.ipv4.ip_conntrack_max=100000**

The next group of rules in this section are important for general system security, and should be entered immediately after the above rules:

```
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD DROP
iptables -I INPUT -i lo -j ACCEPT
iptables -I INPUT -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 22 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p ICMP -j ACCEPT
```

The next group is required for Content Gateway to receive and proxy traffic.

```
iptables -i <CLIENT_NIC> -I INPUT -p tcp --dport 8070 -j
ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 8071 -j ACCEPT
iptables -i <CLIENT_NIC> -I INPUT -p tcp --dport 8080 -j
ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 8081 -j ACCEPT
```

Local Policy Server

Include these rules in your IPTables firewall if the Websense Policy Server runs on the Content Gateway machine.

```
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 40000 -j
ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 55806 -j
ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 55880 -j
ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p udp --dport 55905 -j
ACCEPT
```

Remote Policy Server

Include this rule in your IPTables firewall if the Websense Policy Server does not run on the Content Gateway machine. This is required because Content Gateway has bidirectional communication over ephemeral ports.

Be sure to replace <POLICY Server IP> in the command with the actual IP address of the Policy Server machine.

```
iptables -i <MGMT_NIC> -I INPUT -p tcp -s <POLICY Server IP>
--dport 1024:65535 -j ACCEPT
```

Local Filtering Service

Include these rules in your IPTables firewall if the Websense Filtering Service runs on the Content Gateway machine.

```
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 55807 -j
ACCEPTiptables -i <MGMT_NIC> -I INPUT -p tcp --dport 15868 -
j ACCEPT
```

Remote Filtering Service

Include this rule in your IPTables firewall if the Websense Filtering Service does not run on the Content Gateway machine. This is required because Content Gateway has bidirectional communication over ephemeral ports.

Be sure to replace in the command with the actual IP address of the Filtering Service machine.

```
iptables -i <MGMT_NIC> -I INPUT -s <FILTERING IP Service> -p
tcp --dport 1024:65535 -j ACCEPT
```

Websense Data Security

Include the following rules in your IPTables firewall if Content Gateway is installed as part of Websense Web Security Gateway Anywhere or deployed with Websense Data Security.

```
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 5820 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 8880 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 8888 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 8889 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 9080 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 9090 -j ACCEPT
```

Cluster

Include the following rules in your IPTables firewall if you have multiple instances of Content Gateway in a cluster.

```
iptables -i <CLUSTER_NIC> -I INPUT -p tcp --dport 8086 -j
ACCEPT
iptables -i <CLUSTER_NIC> -I INPUT -p udp --dport 8086 -j
ACCEPT
iptables -i <CLUSTER_NIC> -I INPUT -p tcp --dport 8087 -j
ACCEPT
iptables -i <CLUSTER_NIC> -I INPUT -p udp --dport 8088 -j
ACCEPT
iptables -i <CLUSTER_NIC> -I INPUT -p udp -d
<Multicast_IP_Address> -j ACCEPT
```

Cache hierarchy

Include the following rule in your IPTables firewall if you have multiple instances of Content Gateway in a cache hierarchy.

```
iptables -i <MGMT_NIC> -I INPUT -p udp --dport 3130 -j ACCEPT
```

Transparent proxy

Include the following rule in your IPTables firewall if your network uses transparent proxy.

Include the rule for port 2048 only if your network uses WCCP for transparent proxy.

Include the rule for port 53 and 5353 only if you proxy DNS.

```
iptables -i <CLIENT_NIC> -I INPUT -p tcp --dport 80 -j ACCEPT
iptables -i <CLIENT_NIC> -I INPUT -p tcp --dport 443 -j
ACCEPT
iptables -i <CLIENT_NIC> -I INPUT -p udp --dport 2048 -j
ACCEPT
iptables -i <CLIENT_NIC> -I INPUT -p udp --dport 53 -j ACCEPT
iptables -i <CLIENT_NIC> -I INPUT -p udp --dport 5353 -j
ACCEPT
```

FTP

Include the appropriate rules, below, in your IPTables firewall if you plan to proxy FTP traffic (optional).

```
iptables -i <CLIENT_NIC> -I INPUT -p tcp --dport 21 -j ACCEPT
iptables -i <CLIENT_NIC> -I INPUT -p tcp --dport 2121 -j
ACCEPT
```

Optional features

Include the rule for port 8082, below, to allow gathering of statistics over the overseer port.

Include the rule for port 8083, below, to allow PAC file distribution from the proxy.

Include the rule for port 8085, below, to allow collation of logs for multiple proxies.

```
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 8082 -j ACCEPT
iptables -i <CLIENT_NIC> -I INPUT -p tcp --dport 8083 -j
ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 8085 -j ACCEPT
```

How do I ensure that Content Gateway is properly identified in the network?

Topic 60013 / 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 installed on a stand-alone server, a vital step in the installation process is sometimes skipped with the result that Content Gateway fails to connect to the Websense Web filter policy server or other network services. Sometimes this problem doesn't surface immediately, or surfaces after a second Content Gateway node is added to the network.

To ensure that every Content Gateway node is found and correctly identified on the network, it is essential that on each node the Linux operating system file **/etc/hosts** is

properly configured. The configuration steps are described in the “Checklist” section of the Content Gateway Installation Guide. They are also described below.

NOTE: If there are multiple Websense Content Gateway nodes deployed in a cluster, the cluster name, which is shared by all nodes, cannot be the same as any hostname.

Configuring the /etc/hosts file

On each Content Gateway node, edit the **/etc/hosts** file to include***--on the first line--*** the IP address, fully qualified domain name, and hostname of the node.

1. Log on to the Content Gateway host system as root.
2. Edit **/etc/hosts**. A typical default **/etc/hosts** file looks like:

   ```
   127.0.0.1 localhost.localdomain localhost
   ```
3. Open a new first line and specify the IP address, domain name, and hostname of the system. The format is:

   xxx.xxx.xxx.xxx [FQDN] [hostname]

   where *[FQDN]* is the fully-qualified domain name of the machine, e.g. hostname.subdomain.top-level-domain

   and *[hostname]* is the system hostname.

   For example:

   ```
   10.10.10.10   wcg1.bighost.com         wcg1
   127.0.0.1     localhost.localdomain    localhost
   ```

   The IP address must be static and not served by DHCP. The proxy uses this IP address in features such as transparent authentication and hierarchical caching.

   NOTE: Do not delete the second line (former first line), the one that begins with 127.0.0.1. It specifies the loopback address and is also required.
4. Save and close **/etc/hosts**.

Repeat the above on every Content Gateway node.

Confirming the settings:

To display the configured system hostname, on the Linux command line enter:

```
# hostname
```

To confirm the IP address that is bound to the hostname, on the Linux command line enter:

```
# ping hostname
```

For example:

```
# ping wcg1.bighost.com
```

should return the IP address in line 1 of **/etc/hosts**. It should not return 127.0.0.1.

To test the local loopback address, on the Linux command line enter:

```
# ping localhost
```

This should return 127.0.0.1

To test if the hostname is resolved by DNS (if it is configured), on the Linux command line enter:

```
# nslookup hostname
```

For example:

```
# nslookup wcg1.bighost.com
```

This should return the same IP address as ping.

Note that in some cases it is optional to have the proxy in DNS.

Which Web browsers provide the best user experience with Content Gateway?

Topic 60011 / Updated: 3-June-2010

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

The browsers that provide the most complete support and best user experience are:

Internet Explorer 7 and 8

Mozilla Firefox 2 and 3

Other browsers have limitations, especially when the configured mode is NTLM (Integrated Windows Authentication/Single Sign-on). Transparent NTLM authentication is **not** supported by Google Chrome, Opera or Windows Safari.

Browser	When the client request originates on a **different domain** than the proxy (prompt for credentials)		When the client request originates on the **same domain** as the proxy (transparent authentication; no prompt)	
	HTTP	**HTTPS**	**HTTP**	**HTTPS**
Internet Explorer 7 and 8	Full support			
Mozilla Firefox 2 and 3	Full support			
Google Chrome	NTLM transparent authentication: Not supported. The user is prompted for credentials.			
	Explicit authentication: Supported. The user is prompted for credentials.			

Browser	When the client request originates on a **different domain** than the proxy (prompt for credentials)		When the client request originates on the **same domain** as the proxy (transparent authentication; no prompt)	
	HTTP	**HTTPS**	**HTTP**	**HTTPS**
Opera 10	NTLM transparent authentication: Not supported. The user is prompted for credentials.			
	Explicit authentication:			
	Supported. The user is prompted for credentials.	Not supported.	Supported. The user is prompted for credentials.	Not supported.
Windows Safari 4	NTLM transparent authentication: Not supported. The user is prompted for credentials.			
	Explicit authentication:			
	Supported. The user is prompted for credentials.	Supported. When LDAP authentication is configured, the user is prompted twice for credentials.	Supported. The user is prompted for credentials.	Supported. When LDAP authentication is configured, the user is prompted twice for credentials.

To configure Internet Explorer for Single Sign-On, you must configure the browser to consider the proxy as a local server. Follow these steps in Internet Explorer:

1. Select **Tools > Internet Options > Security > Local intranet > Sites > Advanced**.
2. Enter the URL or IP address of the proxy.
3. Click **Add**.
4. Click **OK** until you have closed all the dialog boxes.

Mozilla Firefox users browsing from the same domain as the proxy may sometimes be prompted multiple times for authentication. The user should configure the browser as follows:

1. Open Firefox and enter "about:config" in the Location bar.
2. Click the "I will be careful I promise" button.
3. In the **Filter** entry field enter "ntlm".
4. Double click "network.automatic-ntlm-auth.trusted-uris" and enter: http://<proxy_name>:8080

   For example: http://XYZProxy1:8080
5. Click OK and close and reopen the browser.

How do I backup and restore the SSL Incident List?

Topic 60015 / Updated: 3-June-2010

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

The SSL Incident List can be backed up and restored on the Linux command line using **sqlite3**.

Start by logging on to the Content Gateway host system and acquiring root privileges.

To back up the Incident List:

1. Change to the Content Gateway SSL database directory:
   ```
   # cd /opt/WCG/sxsuitedb/db
   ```
2. Open “scip3.db” with **sqlite**:
   ```
   # sqlite3 scip3.db
   ```
3. In sqlite, perform the following steps:
   ```
   sqlite> .tables
   sqlite> .output certificate_acl.bak
   sqlite> .dump certificate_acl
   sqlite> .exit
   ```

You now have a backup of the Incident List named “certificate_acl.bak”.

To restore a backup:

1. Change to the Content Gateway SSL database directory and open “scip3.db” with **sqlite3**:
   ```
   # cd /opt/WCG/sxsuitedb/db
   # sqlite3 scip3.db
   ```
2. To replace the current list with the backup list, delete the current list. Skip this step if you want to add the backup list to the current list.
   ```
   sqlite> DELETE FROM certificate_acl
   ```
3. To restore the backup list:
   ```
   sqlite> .read certificate_acl.bak
   sqlite> .exit
   ```
4. In Content Gateway Manager, verify that the Incident List has been restored.

How do I specify in a PAC file a URL that will bypass Content Gateway?

Topic 60023 / Updated: 9-Sept-2010

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

PAC files are easily modified to specify any number of URLs that will bypass the proxy. Such entries are often referred to as *exceptions*.

Most PAC files already have 1 or more exceptions. A common exception is for internal networks. For example:

```
if (isInNet(host, "192.168.0.0", "255.255.0.0")) {return
"DIRECT";}
```

An entry for an external site might look like:

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

Warning

Some versions of Java have had problems with common proxy PAC file functions such as **isInNet()**. Please review the Java open issues in the release notes for the versions of Java used by your client browsers.

Click here to view an example PAC file.

A good Web site for more information and several example PAC files is http://www.findproxyforurl.com/.

Where do I download Content Gateway v7.5.0?

Topic 60024 / Updated: 16-Sept-2010

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

The Web link to the Websense Content Gateway 7.5.0 installer is active, although it no longer appears on the MyWebsense Downloads page.

If you need to install Content Gateway version 7.5.0, please use this link::

http://www.websense.com/downloads/files/v7.5.0/WCG/WebsenseCG75Setup_Lnx.tar.gz