Content Gateway v7.x: Frequently Asked Questions

Topic 60066 | Content Gateway FAQs | Updated: 22-October-2013

Applies To:	Websense Content Gateway v7.x, v7.x Websense Web Security Gateway / Anywhere v7.x, v7.x

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

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

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

How do I backup and restore the SSL Incident List?

Where do I download Content Gateway?

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

Topic 60067 | Content Gateway FAQs | Updated: 22-October-2013

Applies To:	Websense Content Gateway 7.7.x, v7.8.x Websense Web Security Gateway Anywhere 7.7.x, v7.8.x

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.

> ⚠ **Warning**
> 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 v7.6.x sample script, click here

To view a text file version of the v7.7.x sample script, click here.

To view a text file version of the v7.8.x sample script, click here.

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 match only 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 --policy INPUT DROP
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD DROP
iptables -I INPUT -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables --I OUTPUT -o lo -t raw -j NOTRACK
```

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 at startup. To do so, add the following line to **/etc/sysctl.conf**:

```
net.ipv4.ip_conntrack_max=100000
```

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

```
iptables -I INPUT -i lo -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 22 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p ICMP -j ACCEPT
```

Include these rules in v7.7.x deployments to support proxying of HTTPS traffic and access to the SSL Manager:

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

Include these rules to support proxying of HTTP traffic and access to the Content Gateway manager:

```
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 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 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 if the Websense Filtering Service runs on the Content Gateway machine.

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

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

Remote Filtering Service

Include this rule 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 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 17500:17514
-j ACCEPT
```

Cluster

Include the following rules 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 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 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, 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
```

For information on SNMP configuration, see Using SNMP with Content Gateway.

Configuring IP6tables

Content Gateway does not rely on IPv6, but can be configured to meet your other security requirements.

Support is provided for explicit proxy deployments only.

To configure IP6tables firewall, Content Gateway requires that an IPv6 port be open for each protocol that is used (HTTP, HTTPS, FTP, DNS).

Port 8080 is required for Content Gateway to receive and proxy explicit HTTP and HTTPS traffic.

```
ip6tables -i <CLIENT_NIC> -I INPUT -p tcp --dport 8080 -j
ACCEPT
```

Include the rule below if you plan to proxy FTP traffic (optional).

```
ip6tables -i <CLIENT_NIC> -I INPUT -p tcp --dport 2121 -j
ACCEPT
```

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

```
ip6tables -i <CLIENT_NIC> -I INPUT -p udp --dport 53 -j
ACCEPT
ip6tables -i <CLIENT_NIC> -I INPUT -p udp --dport 5353 -j
ACCEPT
```

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

Topic 60068 | Content Gateway FAQs | Updated: 22-October-2013

Applies To:	Websense Content Gateway v7.x Websense Web Security Gateway / Anywhere v7.x

To ensure that every Content Gateway node is found and correctly identified on the network, configure the **/etc/hosts** file on every Content Gateway node in a cluster.

If this is not done, Content Gateway may fail to connect to the Websense Web Security Policy Server or other network services. Sometimes the problem doesn't surface immediately, or surfaces after a second Content Gateway node is added.

> **Important**
> In a Content Gateway 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) 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
```

This 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 60069 | Content Gateway FAQs | Updated: 22-October-2013

Applies To:	Websense Content Gateway 7.8.x Websense Web Security Gateway / Anywhere 7.8.x

Not all Web browsers fully support transparent user authentication.

The following table indicates how a browser responds to an authentication request when Integrated Windows Authentication (IWA) is configured in version 7.8.x. For similar information for other versions, see the Release Notes for that version.

Browser/ Operating System	Internet Explorer (v9, 10 tested)	Firefox	Chrome	Opera (v12.02 tested)	Safari (v6.02 tested)
Windows	Performs transparent authentication	Performs transparent authentication (v21 tested)	Performs transparent authentication (v26, 27 tested)	Falls back to NTLM and prompts for credentials	Falls back to NTLM and prompts for credentials
Mac OS X	Not applicable	Performs transparent authentication (v21 tested)	Browser issue prevents IWA from working (v23 tested)	Not tested	Performs transparent authentication
Red Hat Enterprise Linux, update 6	Not applicable	Performs transparent authentication (v11 tested)	Browser issue prevents IWA from working (v27 tested)	Not tested	Not applicable

✓ **Note**

When prompted for credentials, if the user does not enter a domain name, a “session timeout” error can result, or the user may be re-prompted.

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 60070 | Content Gateway FAQs | Updated: 22-October-2013

Applies To:	Websense Content Gateway v7.x Websense Web Security Gateway / Anywhere v7.x

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:

   For v7.8.x and later:

   ```
   # cd /opt/WCG/config
   ```

   For v7.7.x and earlier:

   ```
   # cd /opt/WCG/sxsuitedb/db
   ```
2. Open the database with **sqlite**:

   For v7.8.x and later:

   ```
   # sqlite3 new_scip3.db
   ```

   For v7.7.x and earlier:

   ```
   # 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 the database with **sqlite3**:

   For 7.8.x and later:

   ```
   # cd /opt/WCG/config
   # sqlite3 new_scip3.db
   ```

   For 7.7.x and earlier:

   ```
   # 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> drop table 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.

Where do I download Content Gateway?

Topic 60071 | Content Gateway FAQs | Updated: 22-October-2013

Applies To:	Websense Content Gateway v7.x Websense Web Security Gateway / Anywhere v7.x

Log on to your MyWebsense account and go to the **Downloads** page. In the **Product** drop down select **Websense Web Security Gateway** or **Web Security Gateway Anywhere**. Locate the release number that you want and click on the “+” icon next to **Websense Content Gateway** to view download details. To begin the download, click **Download**.

To get complete information on installing or upgrading any Websense network security components, visit the Websense Technical Library.