Web Security Gateway

v8.5.x

Content Gateway: Frequently Asked Questions

Revision A

Contents

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

When Content Gateway is deployed on a stand-alone Linux server (not an appliance), 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.

Content Gateway now utilizes iptables, configured during product installation or upgrade, to facilitate interception and redirection of traffic.

- IPTables rules configured outside of Content Gateway Manager must
  - Be inserted *after* Forcepoint rules.
  - Never be added to Forcepoint chains.
- Forcepoint chains and rules should never be edited.
- If customized chains or rules impact the Forcepoint configuration, navigate to `/opt/wcg/bin` and execute the following to re-establish the Forcepoint IPTables chains and rules:

  ```
  netcontrol.sh -r
  ```

While hardening the system is allowed, caution should be taken to avoid interfering with general Content Gateway functionality.

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 from each section that apply to your network.

If the proxy is configured to use multiple NICs, use the -i option (which means “match only if the incoming packet is on the specified interface”) to specify the appropriate NIC for each rule that applies to an 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 Forcepoint Web Security uses for communication, replace the default port shown in the following rules with the custom port you implemented.

All deployments

The following rules are optional and can be used to enhance the security of your Content Gateway deployment.

```
iptables --policy INPUT DROP
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD DROP
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

In addition to the above rules, it is a best practice to increase the size of **nf_conntrack_max** to 100000 to improve performance. Set the size after iptables is started.

- To check the setting, use: **/sbin/sysctl -p**
- To set the value, use:

  ```
  /sbin/sysctl net.nf_conntrack_max=100000
  ```

- If you get the error **"net.nf_conntrack_max" is an unknown key**, you need to add the **ip_conntrack** module to the kernel. Use the command:

  ```
  modprobe ip_conntrack
  ```

The **nf_conntrack_max** value is not be preserved after reboot unless you configure your system to set the value at startup. To do so, add the following line to **/etc/sysctl.conf**:

```
net.nf_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 INPUT -i internal -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p tcp --dport 22 -j ACCEPT
iptables -i <MGMT_NIC> -I INPUT -p ICMP -j ACCEPT
```

Policy Server

All ports needed for communication with a Policy Server are handled internally by the software.

Filtering Service

All ports needed for communication with a Filtering Server machine are handled internally by the software.

Forcepoint Web Security

All ports needed for communication with Forcepoint Web Security are handled internally by the software.

Cluster

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

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

All other ports needed for communication between instanced of Content Gateway are handled internally by the software.

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

All ports needed for transparent proxying are handled internally by the software.

If you proxy DNS, configure port 53 to redirect to port 5353 using Content Gateway Manager.

FTP

All ports needed for FTP proxying are handled internally by the software when FTP is enabled in Content Gateway Manager.

Other features

Communication ports for gathering of statistics over the overseer port, to allow PAC file distribution from the proxy, and for collation of logs for multiple proxies are handled internally by the software.

For information on SIEM integration, see Security Information Event Management (SIEM) Solutions.

Configuring IP6tables

Content Gateway can be configured to support IPv6.

To configure IP6tables firewall, Content Gateway requires that an IPv6 port be open for each protocol that is used for IPv4.

All IPv4 ports that are handed internally by the software are also handled when IPv6 is enabled. Any configurable IPv4 port should be added to IP6tables when IPv6 is enabled in Content Gateway Manager.

For example, include the following rule if you have multiple instances of Content Gateway in a cache hierarchy:

```
ip6tables -i <MGMT_NIC> -I INPUT -p udp --dport 3130 -j ACCEPT
```

Also, the following rules are optional and can be used to enhance the security of your Content Gateway deployment when IPv6 is enabled.

```
ip6tables --policy INPUT DROP
ip6tables --policy OUTPUT ACCEPT
ip6tables --policy FORWARD DROP
ip6tables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

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

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.

Note

If Content Gateway is located on an appliance, there is nothing to do. Configuration of the /etc/hosts is handled automatically as part of initial configuration.

If this is not done, Content Gateway may fail to connect to the Forcepoint 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

Before you begin

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.

Steps

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]`
   [FQDN] is the fully-qualified domain name of the machine, e.g. hostname.subdomain.top-level-domain.
   [hostname] is the system hostname.
   For example:

`10.10.10.10`	`wcg1.example.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.

Next steps

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.example.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.example.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?

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 8.2.x.

Browser/ Operating System	Internet Explorer	Firefox	Chrome	Opera	Safari
Windows	Performs transparent authentication	Performs transparent authentication)	Performs transparent authentication	Performs transparent authentication	Falls back to NTLM and prompts for credentials
Mac OS X	Not applicable	Performs transparent authentication	Falls back to NTLM and prompts for credentials	Falls back to NTLM and prompts for credentials	Performs transparent authentication
Red Hat Enterprise Linux, update 6	Not applicable	Performs transparent authentication	Browser issue prevents IWA from working	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.

Configuring Internet Explorer

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

Steps

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.

Configuring Mozilla Firefox

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:

Steps

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://%3Cproxy_name%3E: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?

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:

Steps

1) Change to the Content Gateway SSL database directory:
   ```
   # cd /opt/WCG/config
   ```
2) Open the database with **sqlite**:
   ```
   # /usr/bin/sqlite3 new_scip3.db
   ```

3) In sqlite, perform the following steps:

```
sqlite> .tables
sqlite> .output certificate_acl.bak
sqlite> .dump certificate_acl
sqlite> .exit
```

Next steps

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

Procedure to restore a backup

Steps

1) Change to the Content Gateway SSL database directory and open the database with **sqlite3**:

```
# cd /opt/WCG/config
# /usr/bin/sqlite3 new_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) Restart the proxy.

5) In the Content Gateway manager, verify that the Incident List has been restored.

How do I download the Content Gateway installer?

Steps

1) Navigate to **support.forcepoint.com** and select the My Account link.

2) Log on to your Forcepoint account, then select the **Downloads** tab.

3) In the **Product** drop-down list, select Forcepoint Web Security.

4) Locate the release number that you want.

5) Click the "**+**" icon next to **Content Gateway** to view download details.

6) To begin the download, click **Download**.

Next steps

To get complete information on installing or upgrading any Forcepoint Web Security components, visit the Technical Library.

Published 06 November 2023