Security Enhancements for Forcepoint Web Security

Forcepoint Web Security and Forcepoint URL Filtering|v8.5.x| April 2022

Use the information provided in this document to enhance the security of your web protection solution. The details provided below allow you to harden your system and ensure you are using the best security measures available.

As a general recommendation, it is always best to install hotfixes as soon as they are available and take regular backups of your configuration.

Port use

The default ports used by Forcepoint on-premises security solutions can be found in this spreadsheet. These ports are used by web, data, and email protection components in both software and appliance deployments.

> **Note**
> The spreadsheet provides the list of default ports. Some may have changed for your deployment at the time of installation.

For web protection solutions, ports for most services require a change to the initialization (INI) file for the component. Dependencies between components may require the change be made in multiple files.

- Instructions for changing the Policy Server and Policy Broker ports can be found in the Server Administration section of the Forcepoint Web Security Administrator Help.
- Use the Web module of the Forcepoint Security Manager to:
  - Configure the Log Server port, and to configure communication with Log Server if the port has changed. See Configuring Log Server.
  - Change port information for transparent identification agents (DC Agent, Logon Agent, RADIUS Agent, or eDirectory Agent). Information for each can be found here.

If instructions for the component that you need to reconfigure are not available, contact Forcepoint Technical Support for assistance.

Event Message Broker Handler port use

The Apache Zookeeper Common/Default Nodes Accessible Without ACL vulnerability has the potential to impact Forcepoint Web Security deployments.

Forcepoint Web Security v8.4 introduced Event Message Broker Handler which was installed with each Policy Broker and used as a load balancer for the Event Message Brokers that were installed with each Policy Server. These components were part of the improvements made for the SIEM Integration feature.

With v8.4 - v8.5.3, Event Message Broker Handler and Event Message Broker communicate over port 55995. With v8.5.4, an Event Message Broker Handler resides with each Event Message Broker and communication is done using port 55992.

To avoid the vulnerability, a deployment of v8.5.4 can include a firewall rule for port 55992, restricting any incoming connection requests.

Deployments of v8.4 - v8.5.3 cannot use a firewall rule. The Event Message Broker Handler must be able to communicate with each Event Message Broker for which it

performs load balancing. Customers using v8.4 - v8.5.3 are advised to upgrade to v8.5.4 and add a firewall rule to avoid this vulnerability.

Securing Web Security components

Access to Web Security components and the machines on which they are installed should be limited to those who have a specific need to configure the general overall deployment of the product. A minimal set of users should be granted root privileges to these servers to restrict access to:

- Files with unencrypted data.
- Temporary files that may contain proprietary information.
- Debug files that may contain unencrypted data.

Secure block pages

Filtering Service can be configured to serve block pages using the HTTPS protocol so that sensitive information is protected.

1. Generate a TLS certificate and key for each instance of Filtering Service that is serving HTTPS block pages.

   See Generating keys and certificates for instructions on how to generate the certificate and key, and how to accept the certificate in the client browser.

   > **Note**
   > Using a self-signed certificate is not advisable, because some of the latest browsers do not allow you to easily override certificate verification. Create a Certificate Authority (CA) first, and then use that to sign the block page certificate.

   The CA certificate can be installed as a trusted root CA on Windows for IE and Chrome browsers, but needs to be installed separately on Firefox. This process is similar to the process used for proxy SSL decryption certificates.
2. Stop Filtering Service.
3. Use a text editor to open the file eimserver.ini (by default, in C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/).
   a. Under the [WebsenseServer] section, add the following values:

      ```
      SSLBlockPage=on
      SSLCertFileLoc=<path to SSL certificate>
      SSLKeyFileLoc=<path to SSL key>
      ```

   b. Save eimserver.ini.

4. Restart Filtering Service.

> **Important**
> If SSLBlockPage is enabled, then Manual Authentication will also use HTTPS, even if Secure Manual Authentication is not enabled.

> **Important**
> If secure block pages are enabled and client browsers are set to proxy through Content Gateway, port 15871 must be included in the **Tunnel Port** or **HTTPS** ports list on the **Configure > Protocols > HTTP** page of Content Gateway manager.

See Secure manual authentication for additional details.

Create and install a new server certificate

To create and install a new server certificate for Forcepoint Security manager, follow the steps outlined in this article.

Note that you may be required to login to Forcepoint Support to view the article.

Create and install a new certificate for Policy Broker

Scanning for security vulnerabilities may show that Policy Broker has a socket which accepts TLS connections but uses a self-signed certificate created by Forcepoint. Although used only for internal communications with Broker clients (other Forcepoint services), it creates the appearance of an insecure server.

Use the information provided in this article to replace the TLS certificate used by Policy Broker with one created by the customer and avoid the appearance of a security hole.

Required external services

In order to function properly, your web protection solution depends on the following external services.

Server name	Purpose
download.forcepoint.com	Subscription verification. Downloads: ● URL and Analytics databases ● Office 365 file ● Certificate Authority (CA) list
appliancehotfix.websense.com	Hotfix downloads for physical and virtual appliances.
appliancepatch.websense.com	Appliance upgrade patch downloads.
hsync-web.mailcontrol.com	(Hybrid deployments) Send policy and configuration data to the cloud.
hlfs-web-a.mailcontrol.com hlfs-web-c.mailcontrol.com hlfs-web-d.mailcontrol.com hlfs-web-e.mailcontrol.com hlfs-web-g.mailcontrol.com hlfs-web-h.mailcontrol.com hlfs-web-j.mailcontrol.com hlfs-web-k.mailcontrol.com hlfs-web-m.mailcontrol.com hlfs-web-n.mailcontrol.com hlfs-web-s.mailcontrol.com	(Hybrid deployments) Download logs from the cloud.

Enable TLSv1.2

Use of the TLSv1.2 protocol is available with the following features and can be enabled using the steps provided.

Always back up a file before making edits.

- Reporting tools running on port 18443.
  1. Navigate to \Websense\Web Security\apache\conf
     a. Use a text editor to open httpd.conf.
     b. Find the following line:

        ```
        SSLProtocol all -SSLv2 -SSLv3
        ```

     c. Replace it with:

```
SSLProtocol -all +TLSv1.2
```

d. Add

```
SSLHonorCipherOrder on
```

e. Find the following line:

```
SSLCipherSuite HIGH:-MD5:!aNULL
```

f. Replace it with:

```
SSLCipherSuite
EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
```

g. Save the close the file.

2. Restart Websense Web Reporting Tools service

- Real-Time Monitor
  1. Navigate to \Websense\Web Security\rtm\tomcat\conf
     a. Use a text editor to open server.xml.
     b. Find the text that begins with <Connector port = ${https port}
     c. Replace the list of ciphers with the following:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

     d. Update the sslEnabledProtocols attribute value to only "TLSv1.2".
     e. Save and close the file.
  2. Restart the RTM Client service.
- Forcepoint Security Manager
  1. Navigate to \Websense\Web Security\tomcat\conf
     a. Use a text editor to open server.xml.
     b. Find the 3 occurrences of “<Connector port = “.
     c. For each, update the sslEnabledProtocols attribute value to only "TLSv1.2". (This value is set, by default, in v8.5.4)
     d. For each, replace the list of ciphers with the following:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

     e. Save your changes and close the file.
  2. Navigate to \EIP Infra\apache\conf\extra (This step is not required for v8.5.4)
     a. Use a text editor to open httpd-ssl.conf.
     b. Redefine the attribute SSL Protocol. (This step is already covered in v8.5.4)

```
SSLProtocol -all +TLSv1.2
```

     c. Save your changes and close the file.

3. Navitgate to \EIP Infra\tomcat\conf.
    a. Use a text editor to open server.xml.
    b. Find the text that begins with <Connector port = 19440”
    c. Replace the list of ciphers with the following:

    ```
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    ```

    d. Add:

    ```
    sslEnabledProtocols="TLSv1.2"
    ```

    e. Save your changes and close the file.
4. Restart the following services:
    - Websense - TRITON Web Security
    - Websense TRITON Web Server
    - TRITON Unified Security Center

- Content Gateway - SSL decryption
    1. Log on to the Content Gateway manager.
    2. Go to the **Configure > SSL > Decryption/Encryption > Inbound** tab.
        a. Under Protocol Settings, make sure only **Use TLSv1.2** is checked, then click **Apply**.
    3. Make the same change on the **Configure > SSL > Decryption/Encryption > Outbound** tab.
- Content Gateway - Rule-Based Authentication

    By defaullt, rule-based authentication supports both TLSv1.1 and TLSv1.2. To support only TLSv1.2, add the following line to the records.config file (located in /opt/WCG/config, by default) and restart Content Gateway.

    ```
    CONFIG proxy.config.sslterm.TLSv11 INT 0
    ```

- Content Gateway - Manage ciphers for UI access

    After v8.5 hotfix 02 or v8.5.3 is installed, TLSv1.2 is enabled in Content Gateway Manager. However, connections continue to use weak ciphers.

    Set the supported cipher list to allow only TLSv1.2 supported ciphers using the following command:

    ```
    /opt/WCG/bin/content_line -s
    proxy.config.admin.supported_cipher_list -v AES256-GCM-
    SHA384,AES256-SHA256,AES128-GCM-SHA256,AES128-SHA256
    ```

    Restart Content Gateway after making this change.

- Block pages -- see *Secure block pages*.
- Policy Engine

    See the information in this KBA for Policy Engine.

- Integrated with DLP

When Forcepoint Web Security is integrated with Forcepoint DLP, review the details found in this KBA for additional security enhancement.

Enable the SameSite Cookie Attribute

The SameSite attribute tells browsers when and how to fire cookies in first- or third-party situations and can be used to prevent the browser from sending the cookies with cross-site requests. The main goal is to mitigate the risk of cross-origin information leakage but this also provides some protection against cross-site request forgery attacks. Valid values for the flag are none, lax, or strict.

Configure this option as follows:

1. Navigate to ..\Websense\Web Security\tomcat\conf\mng and make a backup copy of mng.xml.
2. Use a text editor to open mng.xml.
3. Locate the <\Context> section and add the following before that section:

   ```
   <!-- Add SameSite to the cookies -->
   <CookieProcessor sameSiteCookies="lax" />
   ```

   See the examples below to confirm proper placement.
4. Save your changes and close the file.
5. Locate the mng.xml files in each of these folders:
   - Websense\Web Security\tomcat\conf\Catalina\localhost
   - Websense\Web Security\rtm\tomcat\conf\mng

   and make the same edits.
6. Restart the following services.
   a. Websense TRITON - Web Security
   b. Websense TRITON Web Server
   c. Websense TRITON Unified Security Center
   d. Websense RTM Server

Examples:

Before:

```
<!-- Reporting Service resource -->
  <Environment name="reporting/default/host"
value="${reporting_service.ip}" type="java.lang.String"
description="The reporting service network interface" />
  <Environment name="reporting/default/port"
value="${reporting_service.port}"
type="java.lang.Integer" description="The port of
reporting service" />
</Context>
```

After:

```
<!-- Reporting Service resource -->
  <Environment name="reporting/default/host"
value="${reporting_service.ip}" type="java.lang.String"
description="The reporting service network interface" />
  <Environment name="reporting/default/port"
value="${reporting_service.port}"
type="java.lang.Integer" description="The port of
reporting service" />


  <!-- Add SameSite to the cookies -->
  <CookieProcessor sameSiteCookies="lax" />


</Context>
```

Configure elliptic curves for Forcepoint Security Manger

Elliptic curves, used with some SSL/TLS cipher suites, help provide a secure connection between Forcepoint Security Manager and the browser of the users accessing it. The curves supported with v8.5.4 are:

```
sect163k1 sect163r1 sect163r2 sect193r1 sect193r2
sect233k1 sect233r1 sect239k1 sect283k1 sect283r1
sect409k1 sect409r1 sect571k1 sect571r1 secp160k1
secp160r1 secp160r2 secp192k1 prime192v1 secp224k1
secp224r1 secp256k1 prime256v1 secp384r1 secp521r1
```

The security of the connection between a user's browser and Forcepoint Security Manager can be enhanced by tailoring the list of elliptic curves that are used. In general, curves with a larger bit size are stronger than curves with a smaller bit size. While the default set of elliptic curves is suitable for most purposes, if there is a need to restrict the list of curves to a specific set or to a minimum bit size, follow these steps to change the default configuration.

1. Navigate to \Websense\EIP Infra\apache\conf\extra on the machine where Forcepoint Security Manager resides.
    a. Make a backup of httpd-ssl.conf.
    b. Use a text editor to open httpd-ssl.conf.
    c. Find the line that defines

       `SSLCipherSuite`
    d. To keep the cryptographic configuration details together, add the following lines below that line.

       `SSLOpenSSLConfCmd Curves secp384r1:secp521r1`

```
SSLOpenSSLConfCmd ECDHParameters Automatic
```

The Curves are a colon-separated list of curves you want Forcepoint Security Manager to accept and should be entered as a single line. The ECDHParameters should be set to Automatic.

Additional information on `SSLOpenSSLConfCmd` can be found at this site or here.

e. Save and close the file.

2. Restart the Websense TRITON Web Server service.

   If the service does not start successfully, carefully examine the new configuration lines. The service will fail to start if a curve name is misspelled or not supported.

Using the Active Directory account

See Changing DC Agent, Logon Agent, and User Service permissions in this article to use an Active Directory account with read only privileges.

See the same information for details on using an Active Directory account with Event Log Reader permissions with DC Agent.

Disable DiagClient GUI output

The DiagClient troubleshooting tool allows a customer to remotely view logs and system data using a graphical user interface (GUI).

This exchange is unauthenticated and provides a potential vector by which this data may be exposed to outside sources when the output is sent back to the GUI.

Avoid this problem by removing the DiagClient GUI from the list of logging output destinations.

1. Navigate to the bin directory \Websense\Web Security\bin and locate diagnostics.cfg.
   a. Open the file in a text editor and locate the following line:

      ```
      log4j.rootLogger=ALL, GUI, CONSOLE, FILE
      ```

   b. Remove GUI from the line.

      ```
      log4j.rootLogger=ALL, CONSOLE, FILE
      ```

2. Run WebsenseAdmin –restart to restart Web services.

Repeat these steps on each machine on which a web security solution component has been installed.

With these settings, output will be sent only to the system console and log files. No output will be sent to the DiagClient GUI.

Basic Red Hat Enterprise Linux hardening

For deployments that use Red Hat Enterprise Linux, these resources outline basic Red Hat Enterprise Linux hardening.

- http://www.puschitz.com/SecuringLinux.shtml
- http://www.chekmate.org/wiki/index.php/Hardening_Linux
- http://www.chekmate.org/wiki/index.php/CentOS_Locked_Down_Kickstart

Windows Authentication with SQL Server

Secure communication with SQL Server by using Windows Authentication in place of SQL Authentication.

When installing the web protection solution, when the Forcepoint Management Infrastructure is installed, select Windows Authentication as the authenticaton mode for SQL Server.

1. On the SQL Server screen, select **Use the SQL Server database installed on another machine**, then specify the location and connection credentials for a database server located elsewhere in the network.
2. Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any, and the **Port** to use for SQL Server communication.
   - If you are using a named instance, the instance must already exist.
   - If you are using SQL Server clustering, enter the virtual IP address of the cluster.
3. Specify **Windows Authentication** (a Windows trusted connection), then provide the **User Name** or **Account** and its **Password**.

To use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web module of the Security Manager. See Configuring Apache services to use a trusted connection.

Content Gateway

Harden Content Gateway using the suggestions below.

- *General recommendations for each proxy server*
- *Configure IPTables to harden the host system*
- *Control host access to the Content Gateway manager*

- *Manage client access to the proxy*
- *Import your Root CA*
- *Prevent SSL decryption when Filtering Service is unreachable*
- *Cipher support*
- *Integrated with Forcepoint DLP*

See *Enable TLSv1.2* for additional details on how to configure Content Gateway to use only the TLSv1.2 protocol.

General recommendations for each proxy server

- *Physical Security*
- *Encrypted Traffic*
- *File system contents*
- *Real-Time analysis*
- *Port Usage and Traffic Flow*
- *Externally visible protocols*
- *Basic Red Hat Enterprise Linux hardening*

Physical Security

Administrators should exercise caution in permitting access to the Content Gateway proxy server. Physical access to the server enables users to cycle the power of the server, reboot into single-user mode, and examine the file system. Additionally, with a privilege escalation, a user could also observe user traffic through the proxy.

It is recommended that each proxy server be locked in a small room secured by the Information Technology staff, and a BIOS password should be enabled.

Encrypted Traffic

The proxy software honors the cache control general header field setting of no-cache as defined in the HTTP 1.1 RFC [| section 14]. A website with privacy in mind should set this value by default.

The Content Gateway proxy can be configured to disable caching of HTTPS data for HTTPS pages.

File system contents

Users who obtain root permissions have access to any file on the file system. File information specific to the Content Gateway proxy is listed below.

- The cache, while managed as a raw device, contains user data that is not encrypted.
- /opt/WCG/config/records.config contains:

    - HTTP manager user name and encrypted password
    - LDAP simple bind user name and encrypted password
    - RADIUS Shared Key
    - WCCP v2 Password
    - Anonymous FTP Password
    - Squid Log Collation Secret
    - Product subscription key
    - IP Address/Hostname of Policy Server
    - IP Address/Hostname of LDAP/AD Server
    - Location of SSL cert files
- /opt/WCG/logs/squid.log

Real-Time analysis

User downloads may be cached (for files sent for advanced file analysis) to the disk for examination in real-time. Files may be uncompressed to disk.

Port Usage and Traffic Flow

The following TCP ports should be open on the Content Gateway box, allowed by the host firewall. This can be verified for hosts that use iptables with iptables -L --numeric. For information about configuring IPTables, see *Configure IPTables to harden the host system*, page 14.

- 22 - ssh for command line access
- 23 - ftp
- 80 - http
- 443 - https inbound for transparent proxy deployment
- 2002 - manager connection to NFast SSL accelerator card (internal use only)
- 2004 - manager connection from NFast SSL accelerator card (internal use only)
- 2048 - WCCP (if used)
- 3130 - (UDP) ICP for ICP Cache Heirarchy
- 5002 - alert daemon for NFast SSL accelerator card (internal use only)
- 8070 - https inbound explicit https proxy
- 8080 - Proxy inbound for explicit http proxy
- 8081 - Proxy Manager (http)
- 8082 - Overseer Port **
- 8083 - Autoconfiguration Port **
- 8084 - Process Manager Port **
- 8085 - Logging Server Port **
- 8086 - Clustering Port **

- 8088 - Reliable Service Port **
- 8089 - Multicast Port **
- 8090 - https Outbound (to Microdasys)
- 8190 - Snmp Encapsulation Port (('udp ??)
- 30900 - Download Server for Analytic Db Updates.

See *Port use*, page 2, for additional information about ports used by Forcepoint Web Security. If the components are on a Linux machine, open the required ports in your firewall.

It it recommended that you lock down all ports that are not needed. Proxy features that are not used should have the corresponding ports turned off. Those ports are marked with ** in the list above.

Externally visible protocols

- Wiffle - can be secure and encrypted
- WISP - non-encrypted - contains log messages of who, what, and where (available if Filtering Service is not running on the same server or appliance)

Basic Red Hat Enterprise Linux hardening

These resources outline basic Red Hat Enterprise Linux hardening.

- http://www.puschitz.com/SecuringLinux.shtml
- http://www.chekmate.org/wiki/index.php/Hardening_Linux
- http://www.chekmate.org/wiki/index.php/CentOS_Locked_Down_Kickstart

Configure IPTables to harden the 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. See:

- *Configuring IPTables*
- *All deployments*
- *Policy Server*
- *Filtering Service*
- *Forcepoint Web SecurityCluster*
- *Cache hierarchy*
- *Transparent proxy*
- *FTP*
- *Other features*
- *Configuring IP6tables*

Configuring IPTables

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 but 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
```

Control host access to the Content Gateway manager

Administrators can restrict access to the Content Gateway manager to ensure that only authenticated users can change configuration options and view performance and network traffic statistics.

In addition to using an administrator ID and user accounts, it is possible to control which hosts have access to the Content Gateway manager.

1. In the Content Gateway manager, go to the **Configure > My Proxy > UI Setup > Access** page.
2. In the Access Control area, click **Edit File** to open the configuration file editor for the **mgmt_allow.config** file.
3. Enter information in the fields provided, and then click **Add**. All the fields are described in the UI Setup section of Content Gateway Manager Help..
4. Click **Apply**, and then click **Close**.

Manage client access to the proxy

By default, all clients can access the proxy. Use the following steps to restrict access.

1. In the Content Gateway manger, go to the **Configure > Security > Connection Control**.
2. Click **Edit File** to open the configuration file editor for the ip_allow.config file.
3. Select the default rule which allows all clients and click X to the left of the list to delete the rule.
4. On the same page, add “ip_allow” or “ip_deny” rules based on your internal network requirements.

Import your Root CA

If your organization already has a Root CA, or if you have created a certificate as described here, you can import it into Content Gateway. The certificate must be trusted by all browsers in your organization.

Be sure to back up any new internal Root CA that you import. See Backing up your internal Root CA for details.

To import your Root CA:

1. In the Content Gateway manager, go to the **Configure > SSL > Internal Root CA** > **Import Root CA** tab.
2. Click **Choose File** and browse to select the certificate. The certificate must be in X.509 format and base64-encoded.
3. Click **Choose File** and browse to select the private key. It must correspond to the certificate you selected in Step 2.
   - The certificate and private key format must match.
   - The private key format must match the format required by the importing node (unencrypted or encrypted).

   To verify the certificate and private key format, view the files in a text editor. Use **Backup Root CA** to export the CA from the database.

   Note
   For information on converting the private key format, see:
   - Preparing an Internal Root CA for importing into a FIPS 140-2 enabled node
   - Converting an RSA key type to a PKCS#8 key type
   - Converting an encrypted private key to an RSA key\
4. Enter and confirm the **Passphrase**.
5. Click **Import Root CA**. The imported CA is stored in the SSL configuration database.
6. Restart Content Gateway.

Prevent SSL decryption when Filtering Service is unreachable

Content Gateway will continue to perform SSL decryption on any categories added to the SSL decryption bypass list in Forcepoint Security Manager if communication with Filtering Service is interrupted.

Change this behavior by editing the value of the variable wtg.config.ssl_fail_open in records.config.

1. Log on to the Content Gateway machine as a root user and navigate to /opt/WCG/bin.

2. Run the following to confirm that value of the variable:

   ```
   ./content_line -r wtg.config.ssl_fail_open
   ```

3. If the value is 0 (disabled), run the following to enable the variable.

   ```
   ./content_line -s wtg.config.ssl_fail_open -v 1
   ```

4. Restart Content Gateway.

Cipher support

HTTPS decryption

Prior to v8.5.4, by default, Content Gateway supports 3DES ciphers and 64-bit CBC ciphers for HTTPS (SSL) decryption. Disable support for these ciphers the following steps.

Customers who have installed Content Gateway v8.5.0 Hotfix 10 or Content Gateway v8.5.3 Hotfix 6 do not need to follow this process.

Note that root access is required.

1. **Software**:

   From the command line, navigate to the config folder (/opt/WCG/config, by default).

   Appliance:

   ssh into the Content Gateway and browse to the config directory (/opt/WCG/config, by default).

2. Back up the records.config file.
3. Using a text editor, locate and edit the following in records.config:

   From:

   ```
   CONFIG proxy.config.ssl.server.cipherlist_suffix STRING
   :!ADH:!RC4:!EXP:!DES:@STRENGTH
   ```

   To:

   ```
   CONFIG proxy.config.ssl.server.cipherlist_suffix STRING
   :!ADH:!RC4:!3DES:!EXP:!DES:!IDEA-CBC-SHA:@STRENGTH
   ```

   From:

   ```
   CONFIG proxy.config.ssl.client.cipherlist_suffix STRING
   :!ADH:!RC4:!EXP:!DES:@STRENGTH
   ```

   To:

   ```
   CONFIG proxy.config.ssl.client.cipherlist_suffix STRING
   :!ADH:!RC4:!3DES:!EXP:!DES:!IDEA-CBC-SHA:@STRENGTH
   ```

4. Execute the following command from the bin directory (/opt/WCG/bin, by default):

   ```
   content_line -x
   ```

Support on port 4443

When rule-based authentication is enabled, Content Gateway uses port 4443, which supports 3DES ciphers, as a listening port.

NOTE: Customers who have installed Content Gateway v8.5.0 Hotfix 7 or Content Gateway v8.5.3 Hotfix 3 do not need to follow this process. The workaround below was incorporated into those hotfixes.

To disable 3DES ciphers with rule-based authentication (this requires root access):

1. **Software**:

   From the command line, navigate to the config folder (/opt/WCG/config, by default).

   Appliance:

   ssh into the Content Gateway and browse to the config directory (/opt/WCG/config, by default).
2. Back up the records.config file.
3. Using a text editor, add the following to records.config, then restart the proxy for the changes to take effect:

   ```
   CONFIG proxy.config.sslterm.server.cipher_suite STRING
   @STRENGTH:ALL:!aNULL:!ADH:!RC4:!EXP:!3DES:!EXP:!LOW:!MD5:
   !SSLV2:!NULL
   ```

Integrated with Forcepoint DLP

Encryption is not used with Content Gateway deployments with on-box Web DLP components and the Forcepoint management server when the integration selection is **ICAP**. Use the **Web DLP (integrated on-box)** option for encryption to take place.