BIG-IP® Local Traffic Manager: Applying a Pre-built Cipher String for SSL Negotiation

Version 13.0

Table of Contents

Applying a Pre-built Cipher String for SSL Negotiation

Overview: Using a pre-built cipher string

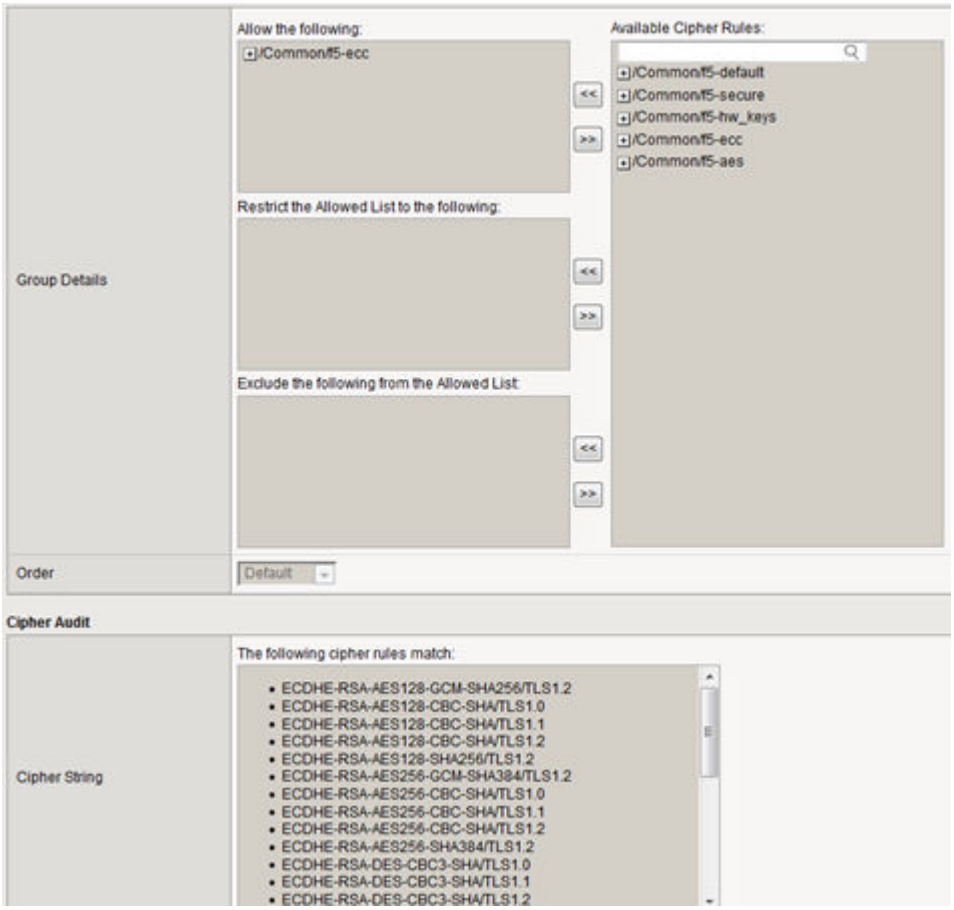
Before the BIG-IP® system can process SSL traffic, you'll need to define the cipher string you want the system to use when negotiating security settings with client or server systems. Typing a raw cipher string on the system is tedious and can easily contain typos. It can also be unsecure, since the cipher string could inadvertently cause the system to negotiate in a way that you didn't intend.

To solve these problems, you can use a pre-built cipher string, known as a cipher group. A *pre-built cipher group* is a named, pre-built set of partial cipher strings (known as *cipher rules*) and a set of instructions that the system uses to create the final cipher string for SSL negotiation.

All pre-built cipher groups are available on the BIG-IP system, ready for you to assign to a Client SSL or Server SSL profile. They are:

- `/Common/f5-default`
- `/Common/f5-aes`
- `/Common/f5-ecc`
- `/Common/f5-hw_keys`
- `/Common/f5-secure`

For example, this illustration shows the pre-built cipher group `/Common/f5-ecc`. The contents of this cipher group are the cipher rule of the same name (`/Common/f5-ecc`), which contains the cipher string `ECDHE:ECDHE_ECDSA` (not shown). You can see a preview of the resulting cipher string in the Cipher Audit area of the screen:



About BIG-IP cipher support

The BIG-IP® system supports a large set of cipher suites that you can choose from to build the cipher string used for security negotiation.

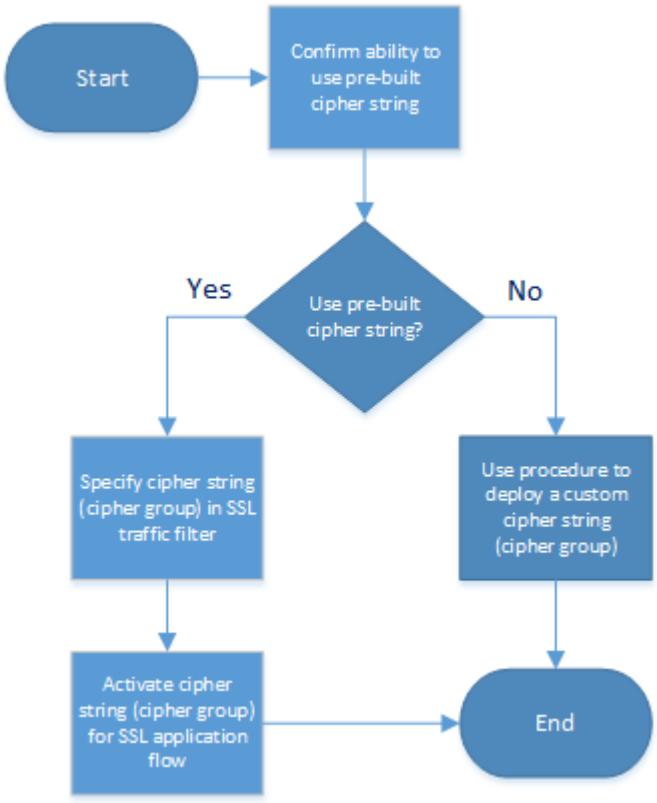
Supported cipher suites include various combinations of encryption algorithms and authentication mechanisms, including RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), and ECDSA (Elliptic Curve Digital signature Algorithm).

The system includes a default cipher string named `DEFAULT`, which contains a subset of the cipher suites that the BIG-IP system supports.

Task summary for configuring a pre-built cipher string

There are a few tasks you need to perform to configure a pre-built cipher string that the BIG-IP® system will use for SSL negotiation.

This illustration shows the order that you need to perform these tasks in.



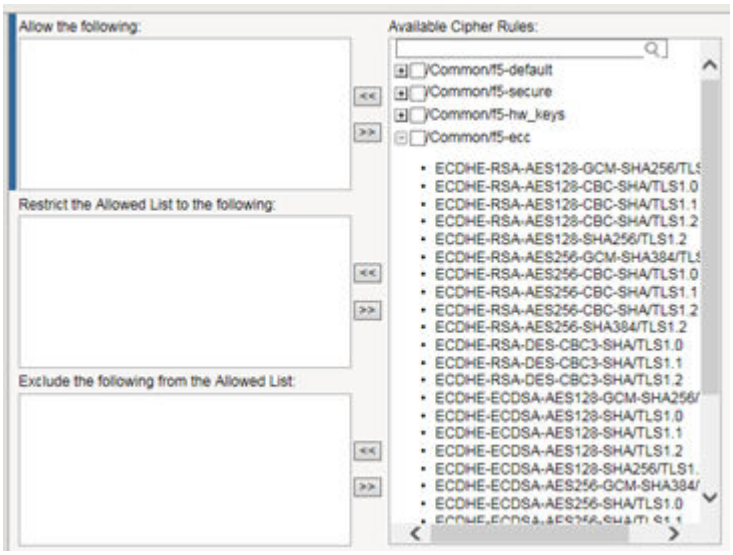
Confirm the ability to use a pre-built cipher string
Specify a cipher string within an SSL traffic filter
Activate a cipher string for an application flow

Confirm the ability to use a pre-built cipher string

Before you configure a cipher string for the BIG-IP® system to use in SSL negotiations with client or server systems, you need to determine whether you can use a pre-built cipher group or whether you'll need to create a custom cipher group. You do this by viewing each pre-built cipher group on the system..

1. On the Main tab, click **Local Traffic** > **Ciphers** > **Groups**.
   The screen displays a list of pre-built cipher groups.
2. In the Name column, click the name of a cipher group.
   For example, click `/Common/f5-ecc`.
3. In the **Available Cipher Rules** list, find the corresponding cipher rule and click the plus sign to view the cipher suites included in the rule.

   For example, this shows the cipher suites included in the pre-built cipher rule named `/Common/f5-ecc`.



4. Click Cancel.
5. As an option, you can repeat this task for any other pre-built cipher groups.

After doing this task, if you found no pre-built cipher group containing all of the cipher suites you need for your cipher string, you'll need to create your own custom cipher group instead.

Specify a cipher string within an SSL traffic filter

Before starting this task, make sure that the relevant traffic filter for managing SSL traffic (either a Client SSL or Server SSL profile) exists on the BIG-IP® system.

You specify the cipher string that the BIG-IP system uses to negotiate security settings with a client or server system, by assigning a cipher group to a Client SSL or Server SSL profile.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client** or **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The Client SSL or Server SSL profile list screen opens.
2. Click the name of a profile.
3. From the **Configuration** list, select **Advanced**.
4. On the right side of the screen, select the **Custom** check box.
5. For the **Ciphers** setting, click **Cipher Group** and from the list, select a cipher group.
6. Click **Update**.

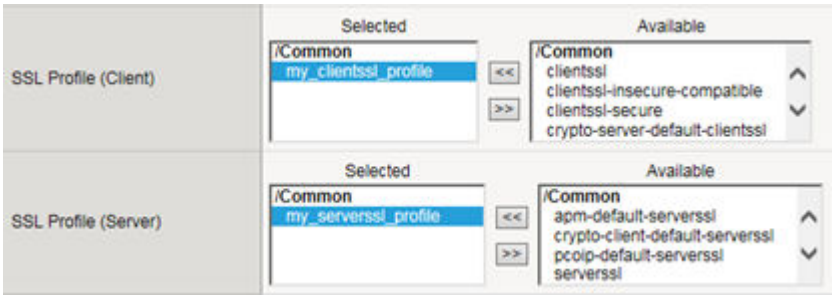
Activate a cipher string for an application flow

Before starting this task, make sure that the virtual server for the relevant SSL application flow exists on the BIG-IP® system.

You activate a cipher string for a specific application flow by assigning a Client SSL or Server SSL profile (or both) to a virtual server. This causes the BIG-IP system to use the cipher group specified in the profile to build the cipher string for negotiating security settings for SSL connections.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of a virtual server.
3. From the **Configuration** list, select **Advanced**.

4. For the **SSL Profile (Client)** and the **SSL Profile (Server)** settings, from the **Available** list, select the name of the SSL profile you previously created, and move the name to the **Selected** list:



   Using the **SSL Profile (Server)** setting is optional.

5. Click **Update** to save the changes.

The BIG-IP system now uses the cipher group specified in an SSL profile to build a cipher string to use when negotiating security for the relevant application flow.

Legal Notices

Legal notices

Publication Date

This document was published on February 13, 2017.

Publication Number

MAN-0656-00

Copyright

Copyright © 2017, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Link Controller Availability

This product is not currently available in the U.S.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a

residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index