Configuration Guide Implementing ITPIN 2018-01 on F5 BigIP Systems

Version: 1.1
Date: July 2019

Disclaimer of Liability
Implementing ITPIN 2018-01 on F5 BigIP Systems- Configuration Guide is intended for exclusive use by Information Technology (IT) Operations personnel working for the Government of Canada and must not be distributed externally.

Intra-Building Network Engineering
Network and End Users Branch (NEUB)
Shared Services Canada (SSC)

Contact Us

For any inquiries or comments about this document, contact the authors Xingyu Sean Zhou (Xingyu.zhou@canada.ca) or James Healey (James.Healey2@canada.ca) or Datacenter Network Application Delivery Controller (DCN ADC) team at Shared Services Canada (SSC): DCN ADC / RCD CDA (SSC/SPC) ssc.dcnadc-rcdcda.spc@canada.ca

Table of Contents

Table of Contents

1. Scope

Information Technology Policy Implementation Notice (ITPIN) 2018-01 directs departments to implement Hypertext Transfer Protocol Secure (HTTPS) for web connections.

ITPIN applies to all publicly accessible Government of Canada websites and web services.

Government internal web sites are out of the scope.

This document provides guidance on configuring F5 BigIP devices as per the recommendation in ITPIN Implementation Guidance. (https://wiki.gccollab.ca/GC_HTTPS_Everywhere/Implementation_Guidance#ITPIN_Implementation_Guidance)

2. ITPIN 2018-01 Requirements

2.1 Requirements overview

The requirements for implementing a secure web connection are listed in Sections 6 of ITPIN 2018-01,

- is configured for HTTPS (and redirected from HTTP)
- has HSTS enabled
- implements TLS 1.2, or subsequent versions, and uses supported cryptographic algorithms and certificates, as outlined in CSE's
    - ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites
    - ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information
- disables known-weak protocols such as all versions of Secure Sockets Layer (SSL) (e.g. SSLv2 and SSLv3) and older versions of TLS (e.g. TLS 1.0 and TLS 1.1), as per CSE ITSP.40.062
- disables known-weak ciphers (e.g. RC4 and 3DES)

2.2 Target Cipher Suites (05/31/2019)

ITPIN Implementation Guidance listed 21 target cipher suites (NEW: 05/31/19), as per the image below,

Target Cipher Suites (NEW: 05/31/19)

Recommended and prioritized (TLS 1.3):

- TLS_AES_256_GCM_SHA384 (5)
- TLS_AES_128_GCM_SHA256 (5)
- TLS_AES_128_CCM_SHA256 (5)

Recommended and prioritized (TLS 1.2):

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Sufficient (Exception Use Only) and prioritized (TLS 1.2):

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (6)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (6)
- TLS_DHE_RSA_WITH_AES_256_CCM (6)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (6)
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (6)
- TLS_DHE_RSA_WITH_AES_128_CCM (6)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (6)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (6)

The following the table compared Full ITSP.40.111 Cipher Suite, Target Cipher Suite, and F5 supported ciphers.

As depicted, BigIP v14 supports 10 out of 21 Target Cipher Suites.

Caveats:

1) While F5 does support the DHE ciphers listed, they are only 1024 bit and are not recommended.
2) The Ciphers for ECDHE_ECDSA require that the certificate applied to the VIP be created as an ECDSA cert instead of RSA.

Full ITSP.40.111 Cipher Suites	Target Cipher Suites	HEX	Coresponding Ciphers (BigIP version)
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	0x1302	TLS13-AES256-GCM-SHA384 (v14+)
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	0x1301	TLS13-AES128-GCM-SHA256 (v14+)
TLS_AES_128_CCM_SHA256	TLS_AES_128_CCM_SHA256	0x1304	N/A
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b	ECDHE-ECDSA-AES128-GCM-SHA256 (any)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	ECDHE-ECDSA-AES256-GCM-SHA384 (any)
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xc0ac	N/A
TLS_ECDHE_ECDSA_WITH_AES_256_CCM	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xc0ad	N/A
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xc023	ECDHE-ECDSA-AES128-SHA256 (any)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xc024	ECDHE-ECDSA-AES256-SHA384 (any)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f	ECDHE-RSA-AES128-GCM-SHA256 (any)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc030	ECDHE-RSA-AES256-GCM-SHA384 (any)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xc027	ECDHE-RSA-AES128-SHA256 (any)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xc028	ECDHE-RSA-AES256-SHA384 (any)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x9e	N/A
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0xa2	N/A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x9f	N/A

TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0xa3	N/A
TLS_DHE_RSA_WITH_AES_128_CCM	TLS_DHE_RSA_WITH_AES_128_CCM	0xc09e	N/A
TLS_DHE_RSA_WITH_AES_256_CCM	TLS_DHE_RSA_WITH_AES_256_CCM	0xc09f	N/A
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x67	N/A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x6b	N/A
TLS_DHE_DSS_WITH_AES_128_CBC_SHA		0x32	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA		0x33	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA		0x38	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA		0x39	
TLS_RSA_WITH_AES_128_GCM_SHA256		0x9c	
TLS_RSA_WITH_AES_256_GCM_SHA384		0x9d	
TLS_RSA_WITH_AES_128_CCM		0xc09c	
TLS_RSA_WITH_AES_256_CCM		0xc09d	
TLS_RSA_WITH_AES_128_CBC_SHA256		0x3c	
TLS_RSA_WITH_AES_256_CBC_SHA256		0x3d	
TLS_RSA_WITH_AES_128_CBC_SHA		0x2f	
TLS_RSA_WITH_AES_256_CBC_SHA		0x35	
TLS_RSA_WITH_3DES_EDE_CBC_SHA		0x0a	
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA		0xc008	
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA		0xc012	
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA		0x13	
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA		0x16	
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		0xc009	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		0xc00a	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		0xc013	

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		0xc014	
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256		0x40	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256		0x6a	

3. Configuring F5 Big-IP

3.1 Configuring HTTPS virtual server

Configuring an HTTPS type of virtual server on BigIP has been a common practice. The following procedures only describe how to configuring the ciphers in SSL profiles (F5 really should rename it to "TLS profiles"!).

Import Note: When BigIP bridges the TLS connection, the ciphers need be configured in both client and server SSL profile.

3.1.1 Cipher String for BigIP up to v13

The following cipher string has been validated on BigIP v12, v13 to be ITPIN compliant. It prefers in the order of cipher strength:

!TLSv1;!TLSv1_1;ECDHE-ECDSA-AES256-GCM-SHA384;ECDHE-ECDSA-AES128-GCM-SHA256;ECDHE-RSA-AES256-GCM-SHA384;ECDHE-RSA-AES128-GCM-SHA256;ECDHE-ECDSA-AES256-SHA;ECDHE-ECDSA-AES128-SHA;ECDHE-RSA-AES256-CBC-SHA;ECDHE-RSA-AES128-CBC-SHA:@STRENGTH

3.1.2 Cipher String for BigIP v14 and above

The following cipher string has been validated to work with BigIP v14 and includes the TLS 1.3 ciphers recommended:

!TLSv1;!TLSv1_1;TLS13-AES256-GCM-SHA384;TLS13-AES128-GCM-SHA256;ECDHE-ECDSA-AES256-GCM-SHA384;ECDHE-ECDSA-AES128-GCM-SHA256;ECDHE-RSA-AES256-GCM-SHA384;ECDHE-RSA-AES128-GCM-SHA256;ECDHE-ECDSA-AES256-SHA;ECDHE-ECDSA-AES128-SHA;ECDHE-RSA-AES256-CBC-SHA;ECDHE-RSA-AES128-CBC-SHA:@STRENGTH

The web service owner may require configuring a subset of Recommended Cipher Suites for stricter cipher security, in that case a more constrained cipher string need be developed and tested. Also some applications may require a loosening of the cipher suite or the allowed TLS version. This must be handled on a case by case basis.

3.2 Configuring SSL Profile on BigIP v12

Note: It is recommended to upgrade to BIG-IP v13 and above to leverage Cipher Groups configuration, see more in the next section.

When configuring SSL profile on BigIP v12, in Ciphers section, input the entire cipher string in the box,

!TLSv1;!TLSv1_1;ECDHE-ECDSA-AES256-GCM-SHA384;ECDHE-ECDSA-AES128-GCM-SHA256;ECDHE-RSA-AES256-GCM-SHA384;ECDHE-RSA-AES128-GCM-SHA256;ECDHE-ECDSA-AES256-SHA;ECDHE-ECDSA-AES128-SHA;ECDHE-RSA-AES256-CBC-SHA;ECDHE-RSA-AES128-CBC-SHA:@STRENGTH

3.3 Configuring SSL Profile on BigIP v13

Since v13 the cipher can be configured with Cipher Groups. For best practice, it is recommended to configure the Cipher Group under the Common partition for following advantages,

- The cipher group can be reused for all other SSL profiles on the system.
- If the ITPIN changed the Target Cipher Suites, it is easier to modify the cipher group than to modify ciphers for each individual SSL profile.

3.3.1 Configuring the cipher rules

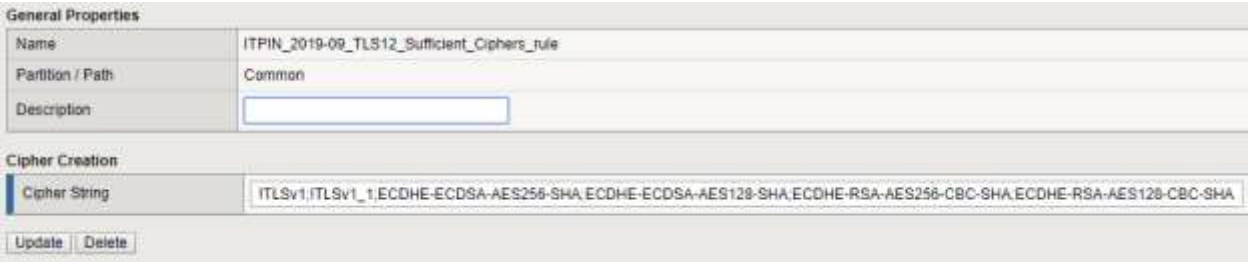
Navigate to Local Traffic > Ciphers > Rules. Create a new cipher.

The first cipher string to accommodate the CSE TLS1.2 "Recommended" list would be:

ECDHE-ECDSA-AES256-GCM-SHA384;ECDHE-ECDSA-AES128-GCM-SHA256;ECDHE-RSA-AES256-GCM-SHA384;ECDHE-RSA-AES128-GCM-SHA256

The second cipher string to accommodate the CSE TLS1.2 "Sufficient" list would be (Note the !TLSv1 and !TLSv1_1):

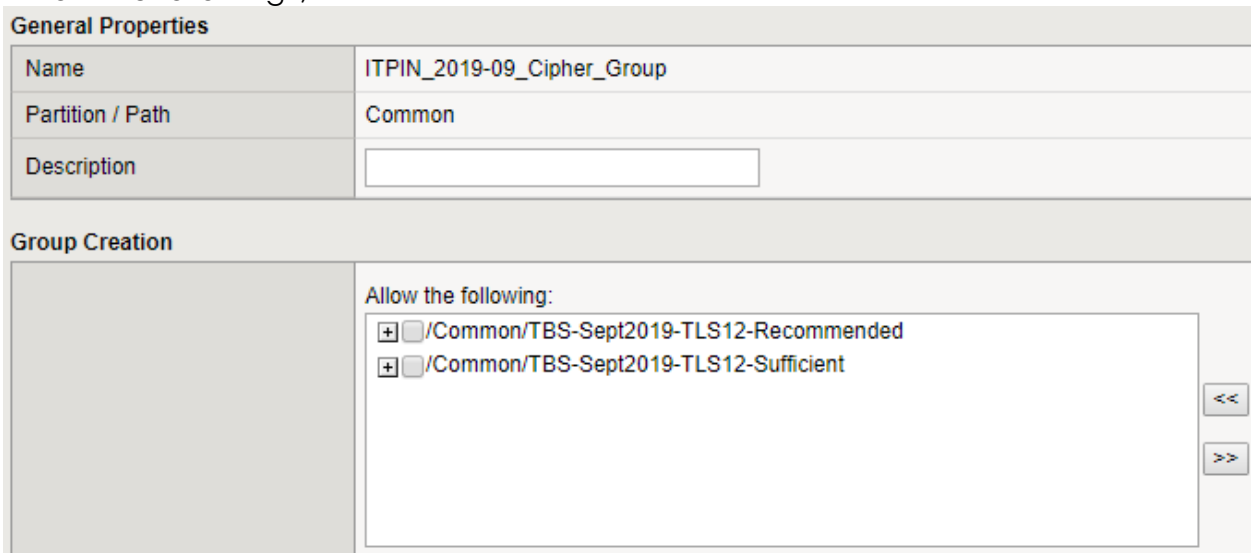
!TLSv1;!TLSv1_1;ECDHE-ECDSA-AES256-SHA;ECDHE-ECDSA-AES128-SHA;ECDHE-RSA-AES256-CBC-SHA;ECDHE-RSA-AES128-CBC-SHA



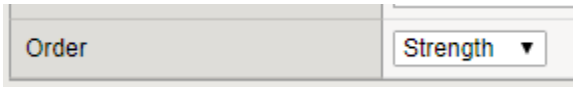
NOTE The sufficient cipher suite allows for a wide range of older clients while maintaining an A+ from SSLLabs and 100% compliance from HTTPS-EVERYWHERE.

3.3.2 Configuring a Cipher Group

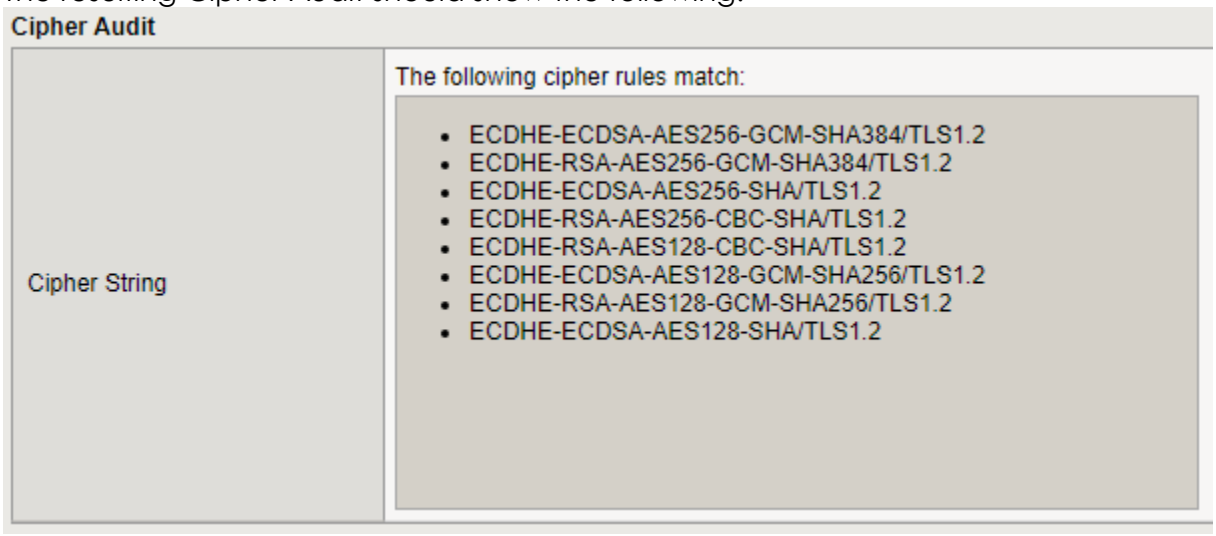
Navigate to Local Traffic > Ciphers > Groups. Move the Cipher Rule created above to "Allow the following",



Change Order to "Strength"



The resulting Cipher Audit should show the following:



Back in the SSL profile, check Cipher Group in Ciphers section, and choose the cipher group created above,


General Properties
Name
SSC_WELCOME_PAGE_PROD_VIP-443_client-ssl
Application
SSC_WELCOME_PAGE_PROD_VIP-443
Partition / Path
SSC_WELCOME_PAGE_PROD/SSC_WELCOME_PAGE_PROD_VIP-443.app
Parent Profile
clientssl
Configuration: Advanced
Mode
Enabled
Certificate Key Chain
/SSC_WELCOME_PAGE_PROD/paz-dt-dev1.bienvenue-welcome.ssc-spc.gc.ca.crt /SSC_WELCOME_PAGE_PROD/paz-dt-dev1.bienvenue-welcome.ssc-spc.gc.ca.key /Common/EntrustChain.crt
Add
Edit
Delete
OCSP Stapling
Notify Certificate Status to Virtual Server
Ciphers
Cipher Group
Cipher String
ITPIN_2018-09_TLS12_Sufficient_Recommended_Ciphers_group

3.4 Configuring SSL Profile on BigIP v14 and Above

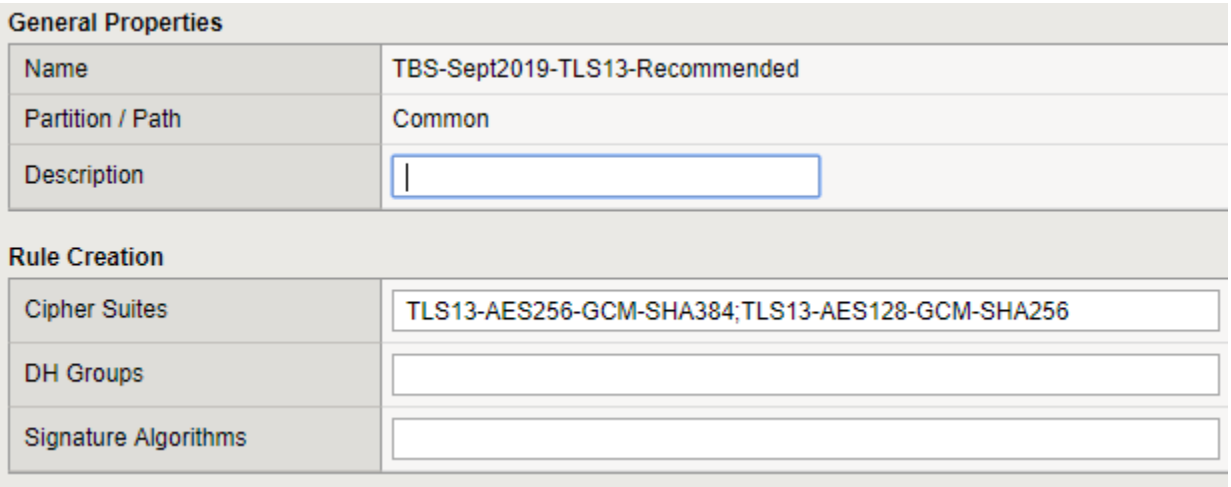
Version 14 of BigIP introduces TLS1.3 ciphers to the suite. So like v13 we chould configure cipher rules and groups in the common partition for use by all.

3.4.1 Configuring the cipher rules

Navigate to Local Traffic > Ciphers > Rules. Create a new cipher.

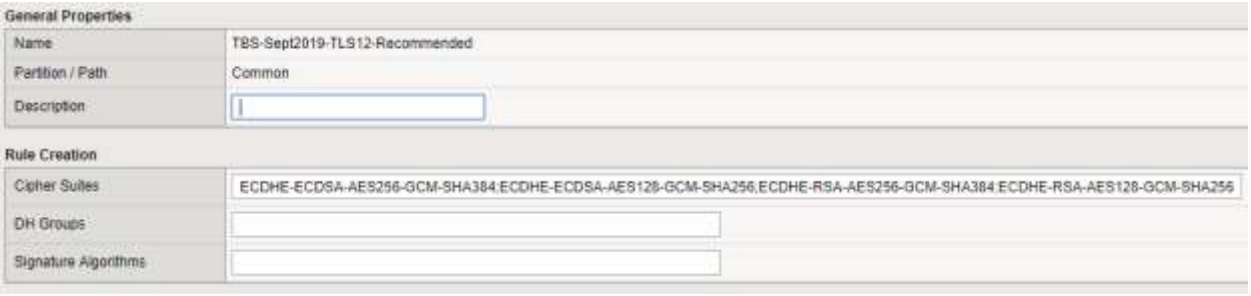
The first cipher string to accommodate the CSE TLS1.3 "Recommended" list would be:

TLS13-AES256-GCM-SHA384;TLS13-AES128-GCM-SHA256



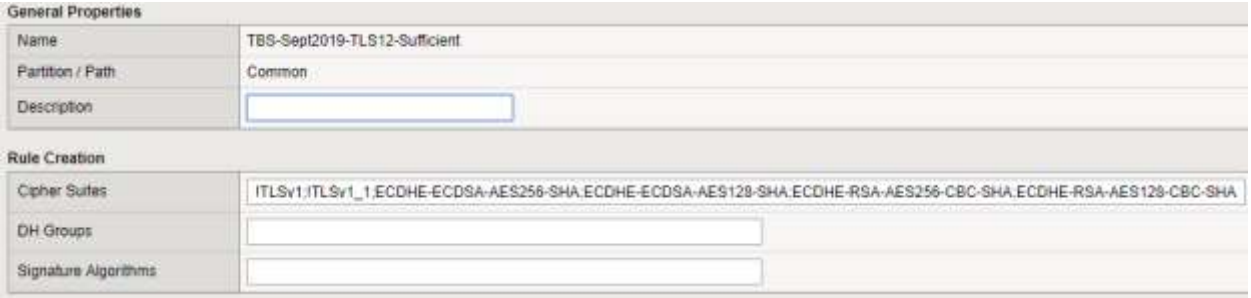
The second cipher string to accommodate the CSE TLS1.2 "Recommended" list would be:

ECDHE-ECDSA-AES256-GCM-SHA384;ECDHE-ECDSA-AES128-GCM-SHA256;ECDHE-RSA-AES256-GCM-SHA384;ECDHE-RSA-AES128-GCM-SHA256



The third cipher string to accommodate the CSE TLS1.2 "Sufficient" list would be (Note the !TLSv1 and !TLSv1_1):

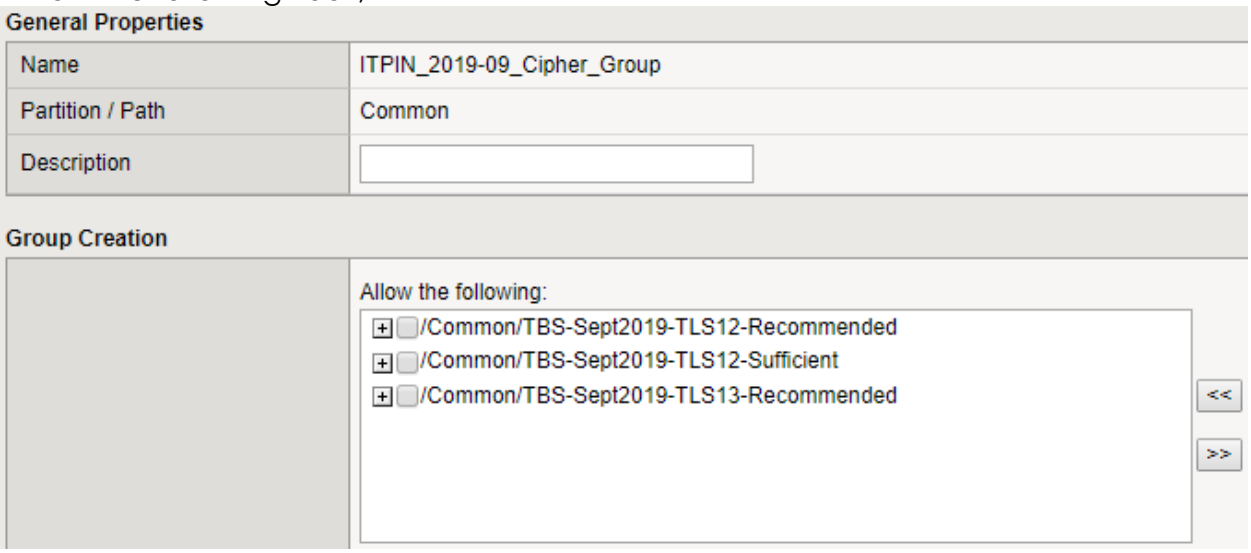
!TLSv1;!TLSv1_1;ECDHE-ECDSA-AES256-SHA;ECDHE-ECDSA-AES128-SHA;ECDHE-RSA-AES256-CBC-SHA;ECDHE-RSA-AES128-CBC-SHA



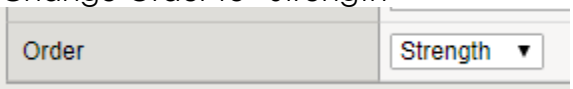
NOTE The sufficient cipher suite allows for a wide range of older clients while maintaining an A+ from SSLLabs and 100% compliance from HTTPS-EVERYWHERE.

3.4.2 Configuring a Cipher Group

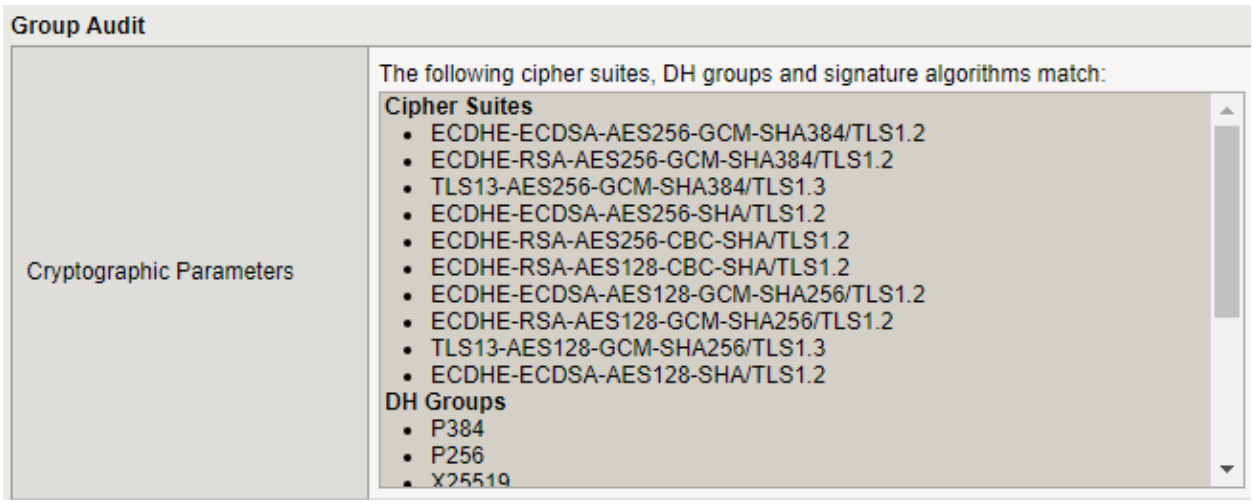
Navigate to Local Traffic > Ciphers > Groups. Move the Cipher Rule created above to "Allow the following" box,



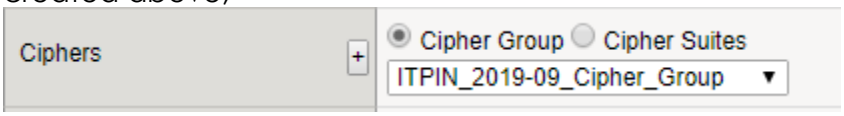
Change Order to "Strength"



The resulting Cipher Audit should show the following:



In SSL profile, check Cipher Group in Ciphers section, and choose the cipher group created above,



3.5 Configuring HTTPS Redirect

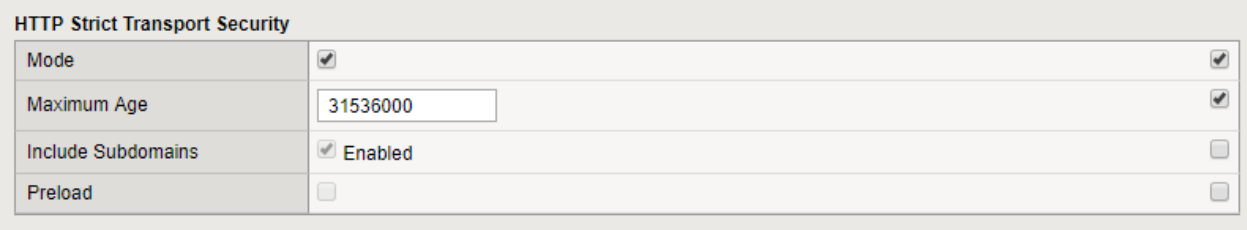
Configuring the virtual server on BigIP to redirect HTTP to HTTPS has been a common practice. The procedures will not be repeated here. It requires to assign a HTTPS redirect iRule on the HTTP virtual server.

3.6 Configuring HSTS

The F5 device can deal with HSTS on behalf of a client if we are doing SSL Offloading. Otherwise the client will have to configure HSTS on the webservers.

To enable HSTS on the F5 the HTTP_Profile for the application must be modified as follows:

Enable Mode
Change Maximum age to 31536000



4 Validation

4.3 Dashboard

TBS has an online dashboard (https://https-everywhere.canada.ca/en/index/) to display if a web site is ITPIN compliance. The dashboard scans overnight on all publically facing government domains.

For example, https://paz-dt-dev1.bienvenue-welcome.ssc-spc.gc.ca/ is showed 100% ITPIN compliant.

4.4 SSLLabs

-

SSLLabs (https://www.ssllabs.com/) is a third party tool can be used to confirm TLS technical details, however the report score such as "A" or "B" cannot be used as a solo measurement for ITPIN compliance.

For example, https://paz-dt-dev1.bienvenue-welcome.ssc-spc.gc.ca/ scores A+ on SSLLabs.