

# 脆弱性(CTX234492及びCTX230238)の対応方法

- 対応方法
- 設定手順
  - GUIでの設定方法
    - CipherSuiteをPFSに限定
  - CLIでの設定方法
    - CipherSuiteをPFSに限定

## 対応方法

利用するCipherSuiteをPFS(DHE/ECDHE)に限定してください。

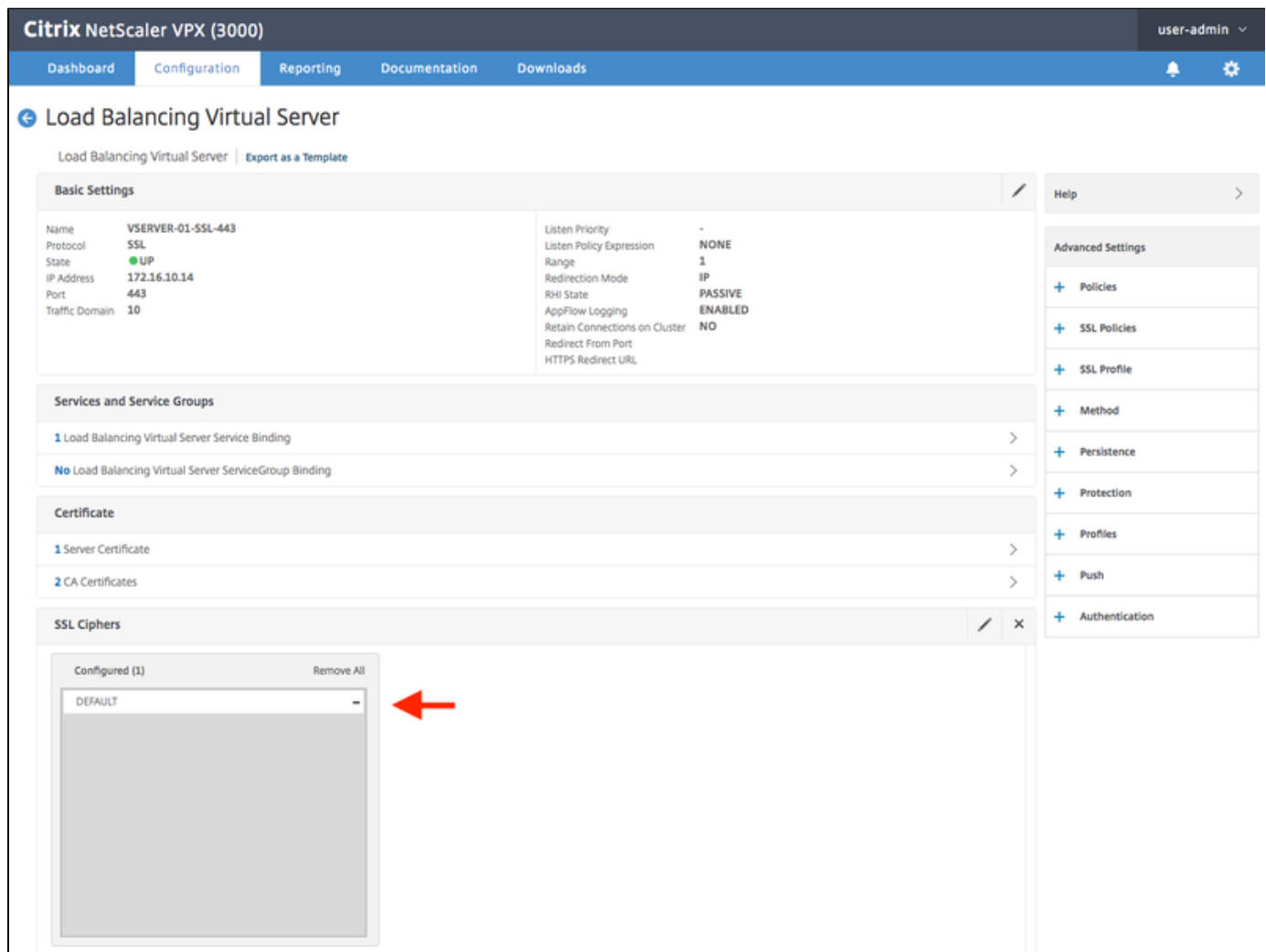
上記を含まないCipherSuiteを使用しないでください。

## 設定手順

### GUIでの設定方法

#### CipherSuiteをPFSに限定

「Traffic Management」 - 「Load Balancing」 - 「Virtual Servers」のVirtual Server設定画面で、SSL Ciphersがdefaultや明示的にDHE/ECDHE以外を利用している場合、該当のCipherSuiteをdisableにします



The screenshot shows the Citrix NetScaler VPX (3000) GUI. The user is logged in as 'user-admin'. The main navigation bar includes Dashboard, Configuration, Reporting, Documentation, and Downloads. The current page is 'Load Balancing Virtual Server' for 'VSERVER-01-SSL-443'. The 'Basic Settings' section shows the server is UP and listening on IP 172.16.10.14, port 443. The 'Services and Service Groups' section shows one binding for 'Load Balancing Virtual Server Service Binding'. The 'Certificate' section shows one server certificate and two CA certificates. The 'SSL Ciphers' section is expanded, showing a list of configured ciphers. A red arrow points to the 'DEFAULT' cipher in the list, indicating it should be disabled.

Basic Settings	
Name	VSERVER-01-SSL-443
Protocol	SSL
State	UP
IP Address	172.16.10.14
Port	443
Traffic Domain	10
Listen Priority	-
Listen Policy Expression	NONE
Range	1
Redirection Mode	IP
RHI State	PASSIVE
AppFlow Logging	ENABLED
Retain Connections on Cluster	NO
Redirect From Port	
HTTPS Redirect URL	

Services and Service Groups	
1	Load Balancing Virtual Server Service Binding
No	Load Balancing Virtual Server ServiceGroup Binding

Certificate	
1	Server Certificate
2	CA Certificates

SSL Ciphers	
Configured (1)	Remove All
DEFAULT	

Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

## Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

### Basic Settings

Name	VSERVER-01-SSL-443	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	UP	Range	1
IP Address	172.16.10.14	Redirection Mode	IP
Port	443	SSL State	PASSIVE
Traffic Domain	10	AppFlow Logging	ENABLED
		Retain Connections on Cluster	NO
		Redirect From Port	
		HTTPS Redirect URL	

### Services and Service Groups

- 1 Load Balancing Virtual Server Service Binding
- No Load Balancing Virtual Server ServiceGroup Binding

### Certificate

- 1 Server Certificate
- 2 CA Certificates

### SSL Ciphers

Configured (8)	Remove All
TLS1.2-AES-256-SHA256	-
TLS1.2-AES-128-SHA256	-
TLS1.2-AES256-GCM-SHA384	-
TLS1.2-AES128-GCM-SHA256	-
TLS1.2-ECDHE-RSA-AES-256-SHA384	-
TLS1.2-ECDHE-RSA-AES-128-SHA256	-
TLS1.2-ECDHE-RSA-AES256-GCM-SHA3...	-
TLS1.2-ECDHE-RSA-AES128-GCM-SHA2...	-

### Advanced Settings

- Polices
- SSL Policies
- SSL Profile
- Method
- Persistence
- Protection
- Profiles
- Push
- Authentication

「SSL Ciphers」の編集ボタンをクリックし、中央の「Add」ボタンをクリックします

SSL Ciphers

Cipher Suites  Cipher Groups

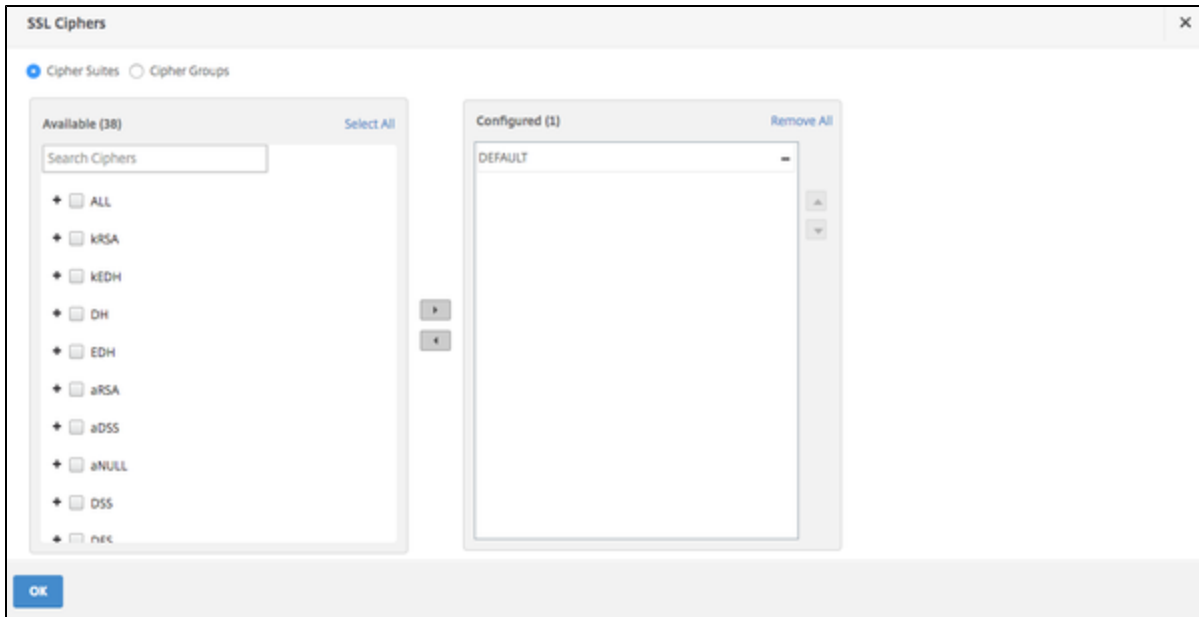
Configured (1) Remove All

DEFAULT

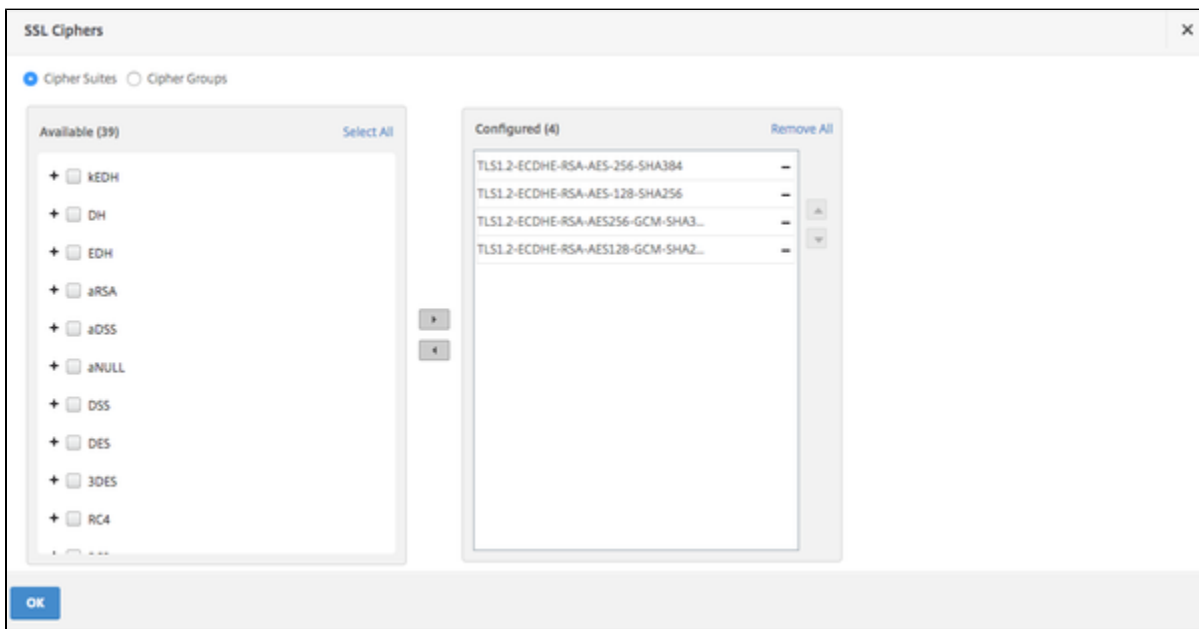
+ Add

OK

左側の「Available」から必要なCipherSuiteを選択し、中央にある右向きボタンをクリックして追加します。  
また右側の「Configured」から、不要なCipherSuiteの右側にある「-」をクリックし削除します。



上記完了後、OKボタンをクリックします（図では、例としてTLS1.2-ECDHE-RSAを選択しております）



設定が正しく反映されていることを確認し、設定を保存します。

Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

## Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

### Basic Settings

Name	VSERVER-01-SSL-443	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	UP	Range	1
IP Address	172.16.10.14	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	10	AppFlow Logging	ENABLED
		Retain Connections on Cluster	NO
		Redirect From Port	
		HTTPS Redirect URL	

### Services and Service Groups

- 1 Load Balancing Virtual Server Service Binding
- No Load Balancing Virtual Server ServiceGroup Binding

### Certificate

- 1 Server Certificate
- 2 CA Certificates

### SSL Ciphers

Configured (4) Remove All

- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA3...
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA2...

### Advanced Settings

- Polices
- SSL Policies
- SSL Profile
- Method
- Persistence
- Protection
- Profiles
- Push
- Authentication

※DHE/ECDHE以外のCipherSuiteを含めたCipherGroupを作成して利用している場合は、CipherGroupを編集します（デフォルトのCipher Groupは編集できないため、新たにグループを作成する必要があります）

「Traffic Management」 - 「SSL」 - 「Cipher Groups」の画面で、利用しているCipher Groupを選択しEditボタンをクリックします。

Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

Search here

Traffic Management / SSL / Cipher Groups

### Cipher Groups

Add Edit Delete Search

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	EXP	Export ciphers
<input type="checkbox"/>	EXPORT	Export ciphers
<input type="checkbox"/>	EXPORT40	Export ciphers with 40bit encryption
<input type="checkbox"/>	EXPORT56	Export ciphers with 56bit encryption
<input type="checkbox"/>	LOW	Low strength ciphers (56bit encryption)
<input type="checkbox"/>	MEDIUM	Medium strength ciphers (128bit encryption)
<input type="checkbox"/>	HIGH	High strength ciphers (168bit encryption)
<input type="checkbox"/>	AES	AES Ciphers
<input type="checkbox"/>	FIPS	FIPS Approved Ciphers
<input type="checkbox"/>	ECDHE	Elliptic Curve Ephemeral DH Ciphers
<input type="checkbox"/>	AES-GCM	Ciphers with Enc algo as AES-GCM
<input type="checkbox"/>	SHA2	Ciphers with MAC algo as SHA-2
<input type="checkbox"/>	DEFAULT_BACKEND	Default cipher list for Backend SSL session
<input type="checkbox"/>	ECDSA	Ciphers with Auth algo as ECDSA
<input checked="" type="checkbox"/>	test_CSGroup	User Defined Cipher Group

Total 40 25 Per Page Page 2 of 2

中央の「Add」ボタンをクリックします

**Citrix NetScaler VPX (3000)**

Dashboard Configuration Reporting Documentation Downloads

## ← Configure Cipher Group

Cipher Group Name  
test\_CSGroup

Configured (8) [Remove All](#)

TLS1.2-ECDHE-RSA-AES-256-SHA3...	-
TLS1.2-ECDHE-RSA-AES-128-SHA2...	-
TLS1.2-ECDHE-RSA-AES256-GCM-...	-
TLS1.2-ECDHE-RSA-AES128-GCM-...	-
TLS1.2-AES-256-SHA256	-
TLS1.2-AES-128-SHA256	-
TLS1.2-AES256-GCM-SHA384	-
TLS1.2-AES128-GCM-SHA256	-

[+ Add](#)

[OK](#) [Close](#)

右側の「Configured」から、不要なCipherSuiteの右側にある「-」をクリックし削除します。

## ← Configure Cipher Group

Cipher Group Name

test\_CSGroup

Available (40)

Select All

Search Ciphers

- +  ALL
- +  DEFAULT
- +  kRSA
- +  kEDH
- +  DH
- +  EDH
- +  aRSA
- +  aDSS
- +  aNULL
- +  rrs



Configured (8)

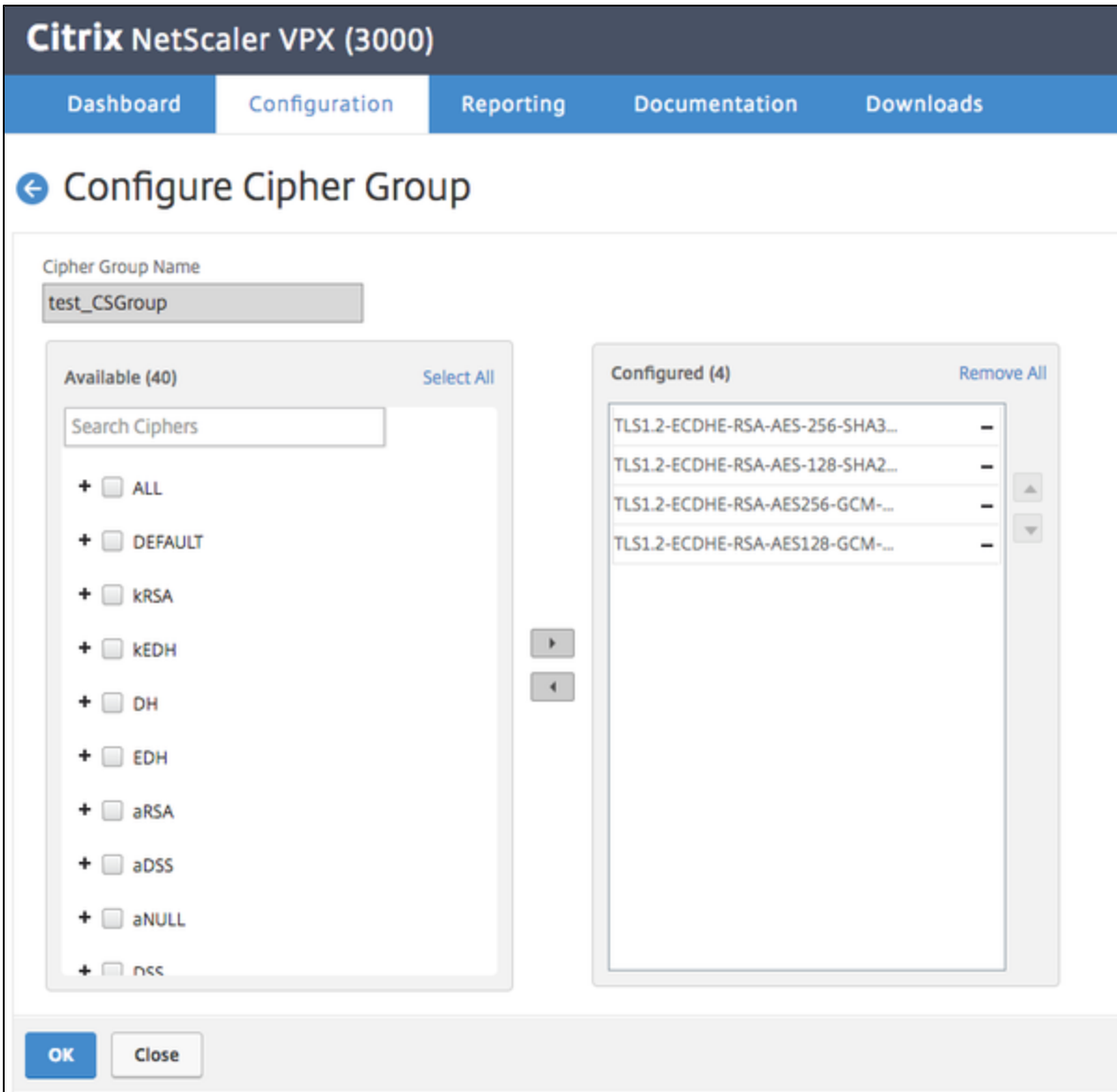
Remove All

- TLS1.2-ECDHE-RSA-AES-256-SHA3... -
- TLS1.2-ECDHE-RSA-AES-128-SHA2... -
- TLS1.2-ECDHE-RSA-AES256-GCM-... -
- TLS1.2-ECDHE-RSA-AES128-GCM-... -
- TLS1.2-AES-256-SHA256 -
- TLS1.2-AES-128-SHA256 -
- TLS1.2-AES256-GCM-SHA384 -
- TLS1.2-AES128-GCM-SHA256 -

OK

Close

上記完了後、OKボタンをクリックします（図では例としてTLS1.2-ECDHE-RSAを選択しております）



CLIでの設定方法

CipherSuiteをPFSに限定

VirtualServerのSSL設定で、CipherSuiteを確認します



DEFAULT

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName DEFAULT
```

CipherSuite

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES-256-SHA256
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES-128-SHA256
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES256-GCM-SHA384
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES128-GCM-SHA256
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES-256-SHA384
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES-128-SHA256
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
```

DEFAULTを利用していた場合、以下のコマンドを実行しDEFAULTの削除、必要なCipherSuiteの設定を行います

```
unbind ssl vserver VSERVER-01-SSL-443 -cipherName DEFAULT
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES-256-SHA384
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES-128-SHA256
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
```

```
bind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
```

個別に指定していた場合、以下のコマンドを実行し不要なCipherSuiteを外します

```
unbind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES-256-SHA256
```

```
unbind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES-128-SHA256
```

```
unbind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-AES256-GCM-SHA384
```

```
unbind ssl vserver VSERVER-01-SSL-443 -cipherName
```

```
TLS1.2-AES128-GCM-SHA256
```

※DHE/ECDHE以外のCipherSuiteを含めたCipherGroupを作成して利用している場合

```
bind ssl cipher test_CSGroup -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384
-cipherPriority 1
bind ssl cipher test_CSGroup -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256
-cipherPriority 2
bind ssl cipher test_CSGroup -cipherName
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 3
bind ssl cipher test_CSGroup -cipherName
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 4
bind ssl cipher test_CSGroup -cipherName TLS1.2-AES-256-SHA256
-cipherPriority 5
bind ssl cipher test_CSGroup -cipherName TLS1.2-AES-128-SHA256
-cipherPriority 6
bind ssl cipher test_CSGroup -cipherName TLS1.2-AES256-GCM-SHA384
-cipherPriority 7
bind ssl cipher test_CSGroup -cipherName TLS1.2-AES128-GCM-SHA256
-cipherPriority 8
```

以下のコマンドを実行し不要なCipherSuiteを外します

```
unbind ssl cipher test_CSGroup -cipherName TLS1.2-AES-256-SHA256
unbind ssl cipher test_CSGroup -cipherName TLS1.2-AES-128-SHA256
unbind ssl cipher test_CSGroup -cipherName TLS1.2-AES256-GCM-SHA384
unbind ssl cipher test_CSGroup -cipherName TLS1.2-AES128-GCM-SHA256
```