

# 脆弱性(CTX230612)の対応方法

- 対応方法
- 設定手順
  - GUIでの設定方法
    - realserverに対するクライアント証明書の認証解除
    - CipherSuiteのDHEを無効化
  - CLIでの設定方法
    - realserverに対するクライアント証明書の認証解除
    - CipherSuiteのDHEを無効化

## 対応方法

NetScalerとrealserver間の認証にクライアント証明書を利用している場合、以下のいずれか2点の対応を実施ください。

- クライアント証明書の利用を中止する
- DHEのCipherSuiteを利用しない

## 設定手順

### GUIでの設定方法

#### realserverに対するクライアント証明書の認証解除

realserver側に指定されたwebサーバの設定については、環境にあわせて別途変更が必要です。

「Traffic Management」 - 「Load Balancing」 - 「Services」 のLoad Balancing Service設定画面でclient証明書の認証を利用している場合、certificateにClient証明書が登録されています

**Citrix NetScaler VPX (3000)** user-admin

Dashboard Configuration Reporting Documentation Downloads

### Load Balancing Service

**Basic Settings**

Service Name	test1	Traffic Domain	LD
Server Name	TD_10_1.1.1.1	Number of Active Connections	-
IP Address	1.1.1.1	Hash ID	-
Server State	DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	443	Cache Type	SERVER
Comments		Cacheable	NO
Monitoring Connection Close Bit	NONE	Health Monitoring	YES
		AppFlow Logging	ENABLED

**Service Settings**

Sure Connect	OFF	Use Source IP Address	YES
Surge Protection	YES	Client Keep-Alive	NO
Use Proxy Port	ENABLED	TCP Buffering	NO
Down State Flush	NO	Compression	NO
Access Down	NO	Insert Client IP Address	DISABLED
		Header	CLIENTIP

**Monitors**

1 Service to Load Balancing Monitor Binding

**SSL Parameters**

Enable DH Param	DISABLED	SSL Redirect Port Rewrite	DISABLED	OCSP Stapling	DISABLED
Refresh Count	0	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
File Path		Redirect URL		SSLv2 URL	
Enable DH Key Expire Size Limit	DISABLED	Send Close-Notify	YES	SSLv2	DISABLED
Enable Ephemeral RSA	DISABLED	SNI Enable	DISABLED	SSLv3	DISABLED
Refresh Count	0	HSTS		TLSv1	DISABLED
Enable Session Reuse	ENABLED	Max Age		TLSv1.1	DISABLED
Time-out	300	Include Subdomains		TLSv1.2	ENABLED
SSL Redirect	DISABLED	Enable Server Authentication	DISABLED		
DTLS Profile	-	Client Authentication	DISABLED		
Strict Signature Digest Check	DISABLED	Client Certificate			

**SSL Ciphers**

Configured (8)

- Remove All
- TLSSL2-ECDHE-RSA-AES-256-SHA384
- TLSSL2-ECDHE-RSA-AES-128-SHA256
- TLSSL2-ECDHE-RSA-AES256-GCM-SHA384
- TLSSL2-ECDHE-RSA-AES128-GCM-SHA256
- TLSSL2-DHE-RSA-AES-256-SHA256
- TLSSL2-DHE-RSA-AES-128-SHA256
- TLSSL2-DHE-RSA-AES256-GCM-SHA384
- TLSSL2-DHE-RSA-AES128-GCM-SHA256

**Certificate**

- 1 CA Certificates
- 1 Client Certificate

Done

上記のClient Certificateの箇所をクリックすると下図に遷移します

**Citrix NetScaler VPX (3000)** user-admin

Dashboard Configuration Reporting Documentation Downloads

### Load Balancing Service

**SSL Service Client Certificate Binding**

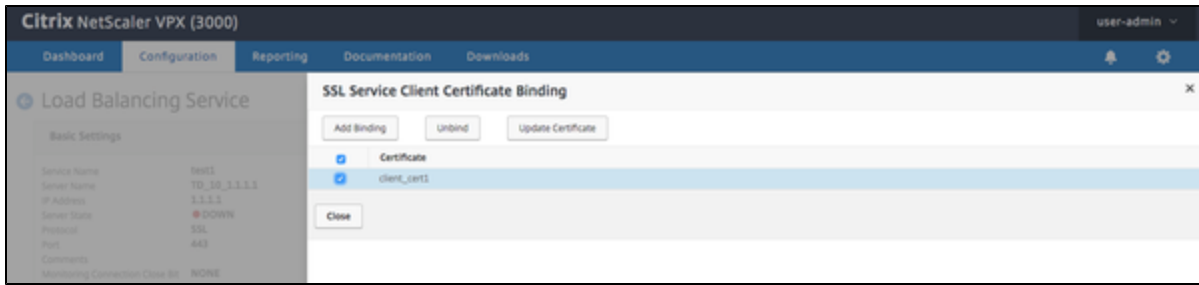
Add Binding Unbind Update Certificate

Certificate

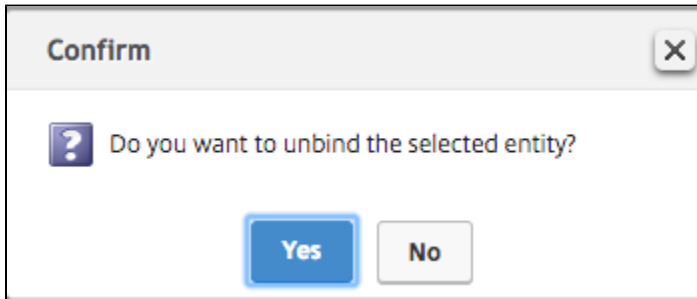
client\_cert1

Close

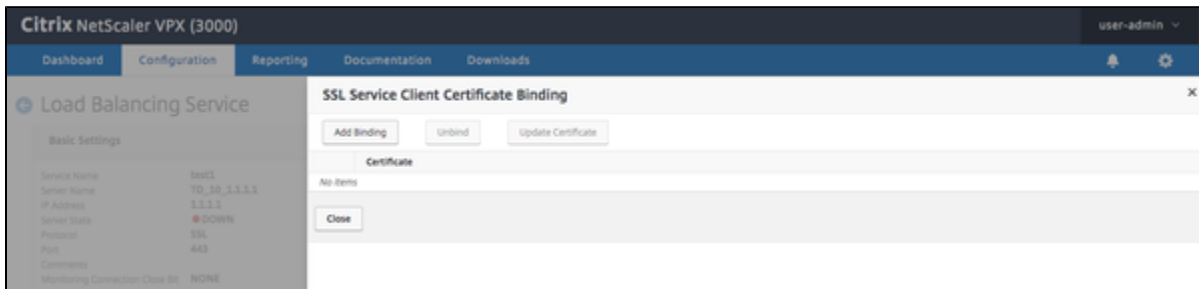
クライアント証明書を選択し、Unbindボタンをクリックします



下記メッセージが表示されたらYesを選択します



Unbindされていることを確認し、Closeボタンをクリックします



Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

## Load Balancing Service

### Basic Settings

Service Name	test1	Traffic Domain	10
Server Name	TD_10_1.1.1.1	Number of Active Connections	-
IP Address	1.1.1.1	Hash ID	-
Server State	DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	443	Cache Type	SERVER
Comments		Cacheable	NO
Monitoring Connection Close Bit	NONE	Health Monitoring	YES
		AppFlow Logging	ENABLED

### Service Settings

Secure Connect	OFF	Use Source IP Address	YES
Surge Protection	YES	Client Keep-Alive	NO
Use Proxy Port	ENABLED	TCP Buffering	NO
Down State Flush	NO	Compression	NO
Access Down	NO	Insert Client IP Address Header	DISABLED (RENT-IP)

### Monitors

Service to Load Balancing Monitor Binding

### SSL Parameters

Enable DH Param	DISABLED	SSL Redirect Port Rewrite	DISABLED	OCSP Stapling	DISABLED
Refresh Count	0	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
File Path		Redirect URL		SSLv2 URL	
Enable DH Key Expire Size Limit	DISABLED	Send Close-Notify	YES	SSLv3 URL	DISABLED
Enable Ephemeral RSA	DISABLED	SNI Enable	DISABLED	SSLv3	DISABLED
Refresh Count	0	HSTS		TLSv1	DISABLED
Enable Session Reuse	ENABLED	Max-Age		TLSv1.1	DISABLED
Time-out	300	Include Subdomains		TLSv1.2	ENABLED
SSL Redirect	DISABLED	Enable Server Authentication			
DTLS Profile	-	Client Authentication	DISABLED		
Strict Signature Digest Check	DISABLED	Client Certificate			

### SSL Ciphers

Configured (8) Remove All

- TLSSL2-ECDH-RSA-AES-256-SHA384
- TLSSL2-ECDH-RSA-AES-128-SHA256
- TLSSL2-ECDH-RSA-AES256-GCM-SHA384
- TLSSL2-ECDH-RSA-AES128-GCM-SHA256
- TLSSL2-DHE-RSA-AES-256-SHA256
- TLSSL2-DHE-RSA-AES-128-SHA256
- TLSSL2-DHE-RSA-AES256-GCM-SHA384
- TLSSL2-DHE-RSA-AES128-GCM-SHA256

### Certificate

CA Certificates

No Client Certificate

Done

## CipherSuiteのDHEを無効化

「Traffic Management」 - 「Load Balancing」 - 「Services」 のLoad Balancing Service設定画面で、SSL Ciphersがdefaultや明示的にDHEを利用している場合、DHEのCipherSuiteをdisableにします

### Load Balancing Service


Basic Settings	
Service Name	test1
Server Name	TD_10_1.1.1.1
IP Address	1.1.1.1
Server State	DOWN
Protocol	SSL
Port	443
Comments	
Monitoring Connection Close Bit	NONE
Traffic Domain	10
Number of Active Connections	-
Hash ID	-
Server ID	None
Clear Text Port	-
Cache Type	SERVER
Cacheable	NO
Health Monitoring	YES
AppFlow Logging	ENABLED

Service Settings	
Sure Connect	OFF
Surge Protection	OFF
Use Proxy Port	YES
Down State Flush	ENABLED
Access Down	NO
Use Source IP Address	YES
Client Keep-Alive	NO
TCP Buffering	NO
Compression	NO
Insert Client IP Address Header	DISABLED
	client-ip

Monitors
1 Service to Load Balancing Monitor Binding

SSL Parameters	
Enable DH Param	DISABLED
Refresh Count	0
File Path	
Enable DH Key Expire Size Limit	DISABLED
Enable Ephemeral RSA	DISABLED
Refresh Count	0
Enable Session Reuse	ENABLED
Time-out	300
SSL Redirect	DISABLED
DTLS Profile	-
Strict Signature Digest Check	DISABLED
SSL Redirect Port Rewrite	DISABLED
Enable Cipher Redirect	DISABLED
Redirect URL	
Send Close-Notify	YES
SNI Enable	DISABLED
HSTS	
Max Age	
Include Subdomains	
Enable Server Authentication	DISABLED
Client Authentication	DISABLED
Client Certificate	
OCSP Stapling	DISABLED
SSLv2 Redirect	DISABLED
SSLv2 URL	
SSLv2	DISABLED
SSLv3	DISABLED
TLSv1	DISABLED
TLSv1.1	DISABLED
TLSv1.2	ENABLED

SSL Ciphers
Configured (1) <span>Remove All</span>
DEFAULT



- Help
- Advanced Settings
  - Thresholds & Timeouts
  - Profiles
  - Policies
  - SSL Profile
  - SSL Policies
  - ECC Curve

## Load Balancing Service

## Basic Settings

Service Name	test1	Traffic Domain	10
Server Name	TD_10_1.1.1.1	Number of Active Connections	-
IP Address	1.1.1.1	Hash ID	-
Server State	● DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	443	Cache Type	SERVER
Comments		Cacheable	NO
Monitoring Connection Close Bit	NONE	Health Monitoring	YES
		Appflow Logging	ENABLED

## Service Settings

Sure Connect		Use Source IP Address	YES
Surge Protection	OFF	Client Keep-Alive	NO
Use Proxy Port	YES	TCP Buffering	NO
Down State Flush	ENABLED	Compression	NO
Access Down	NO	Insert Client IP Address	DISABLED
		Header	client-ip

## Monitors

1 Service to Load Balancing Monitor Binding

## SSL Parameters

Enable DH Param	DISABLED	SSL Redirect Port Rewrite	DISABLED	OCSP Stapling	DISABLED
Refresh Count	0	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
File Path		Redirect URL		SSLv2 URL	
Enable DH Key Expire Size Limit	DISABLED	Send Close-Notify	YES	SSLv2	DISABLED
Enable Ephemeral RSA	DISABLED	SNI Enable	DISABLED	SSLv3	DISABLED
Refresh Count	0	HSTS		TLSv1	DISABLED
Enable Session Reuse	ENABLED	Max Age		TLSv1.1	DISABLED
Time-out	300	Include Subdomains		TLSv1.2	ENABLED
SSL Redirect	DISABLED	Enable Server Authentication	DISABLED		
DTLS Profile	-	Client Authentication	DISABLED		
Strict Signature Digest Check	DISABLED	Client Certificate			

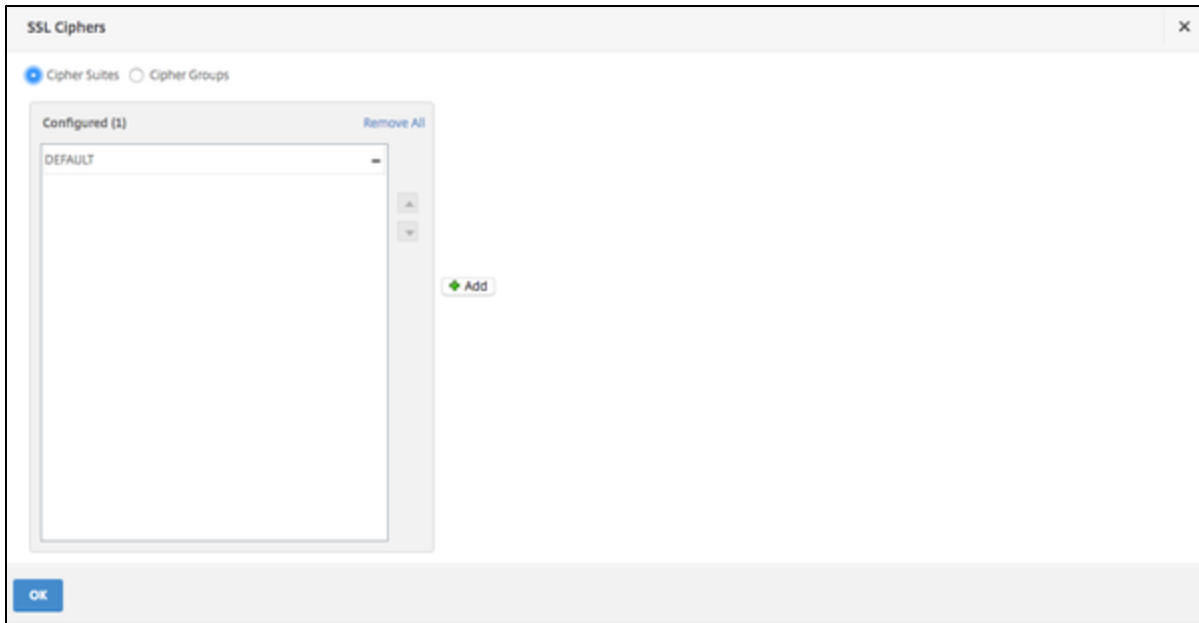
## SSL Ciphers

Configured (8)

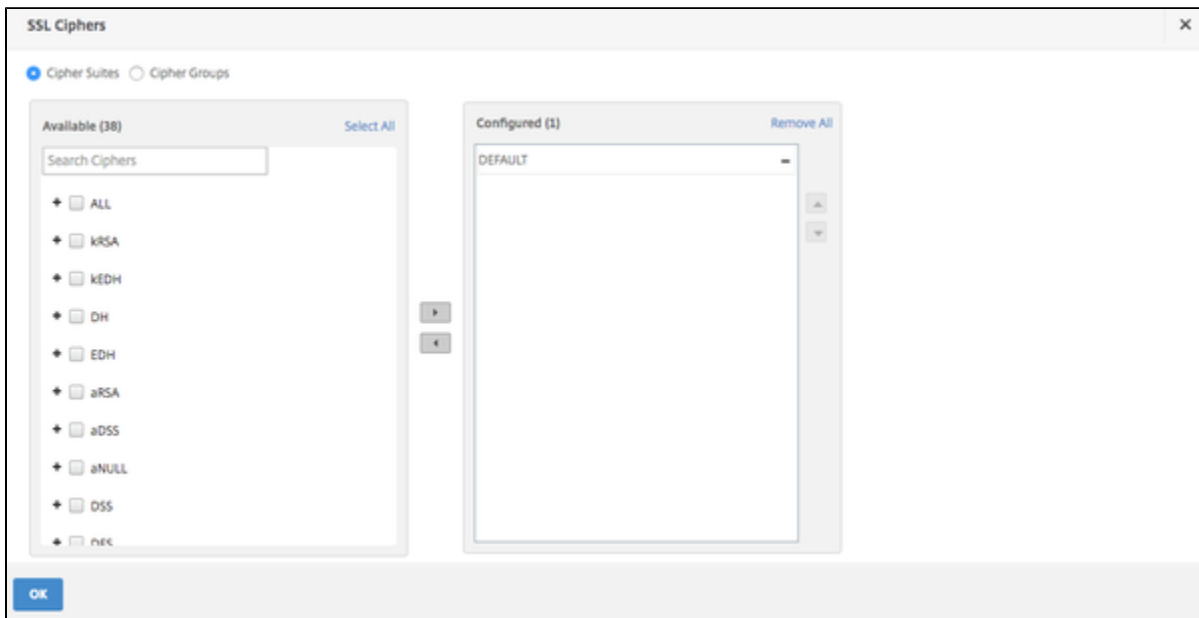
Remove All

- TLSt1.2-ECDHE-RSA-AES-256-SHA384
- TLSt1.2-ECDHE-RSA-AES-128-SHA256
- TLSt1.2-ECDHE-RSA-AES256-GCM-SHA3...
- TLSt1.2-ECDHE-RSA-AES128-GCM-SHA2...
- TLSt1.2-DHE-RSA-AES-256-SHA256
- TLSt1.2-DHE-RSA-AES-128-SHA256
- TLSt1.2-DHE-RSA-AES256-GCM-SHA384
- TLSt1.2-DHE-RSA-AES128-GCM-SHA256

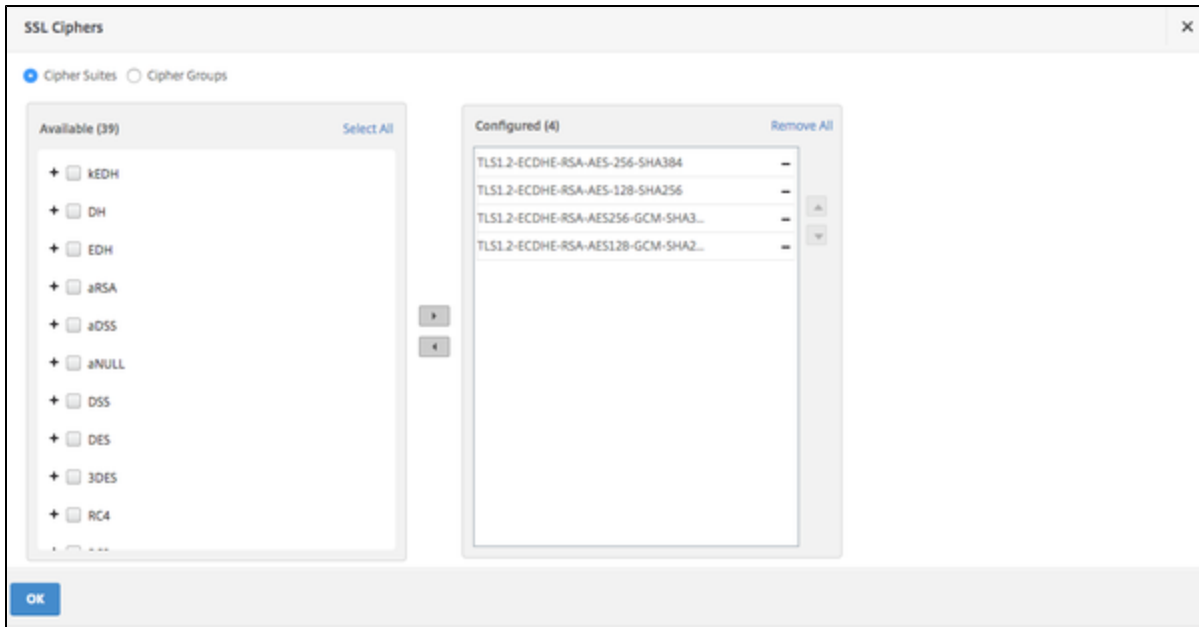
「SSL Ciphers」の編集ボタンをクリックし、中央の「Add」ボタンをクリックします



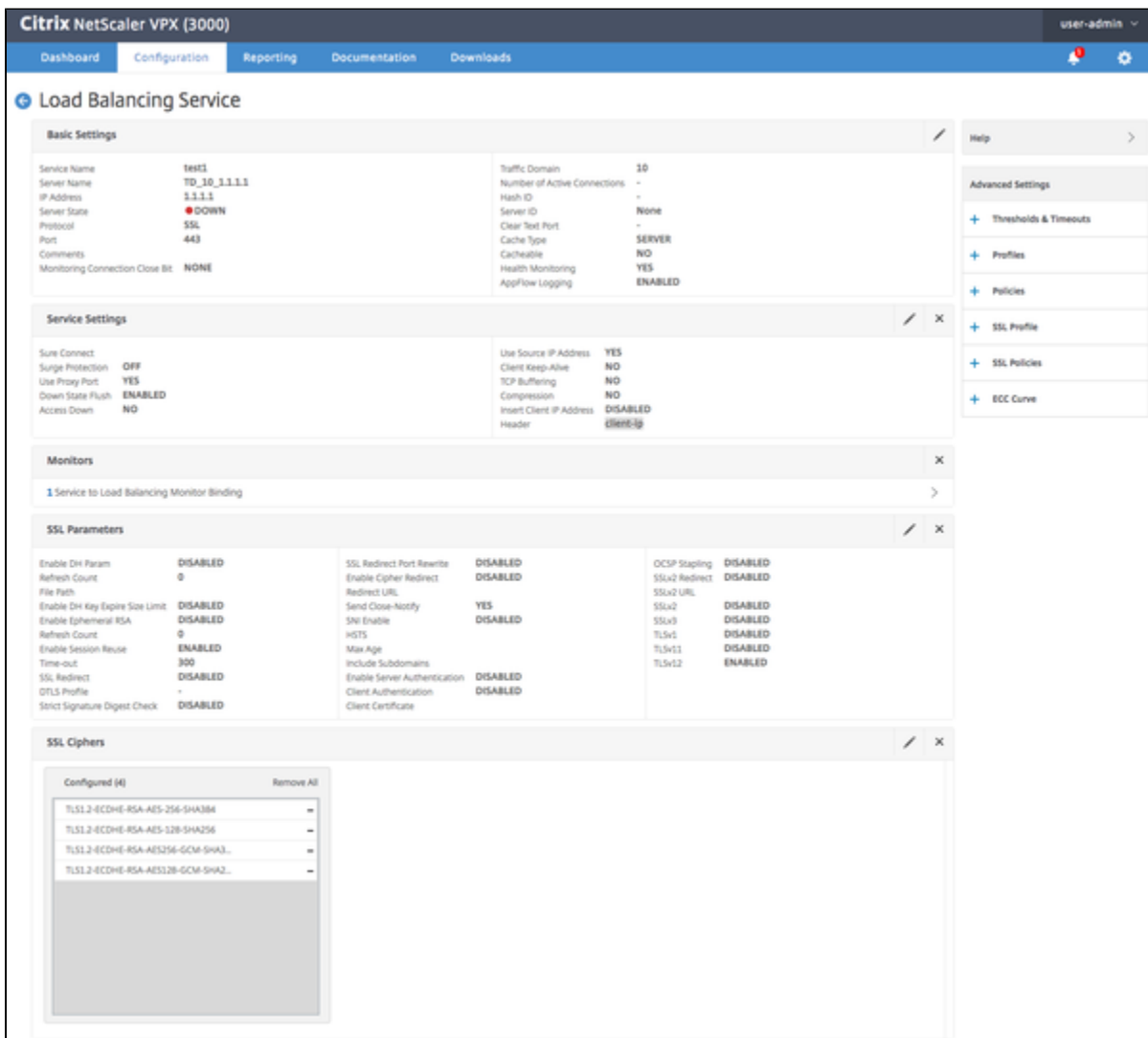
左側の「Available」から必要なCipherSuiteを選択し、中央にある右向きボタンをクリックして追加します。  
また右側の「Configured」から、不要なCipherSuiteの右側にある「-」をクリックし削除します。



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を選択している）



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。





※DHE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。

The screenshot shows the Citrix NetScaler VPX (3000) Configuration page for Cipher Groups. The page has a navigation menu on the left with categories like System, AppExpert, and Traffic Management. The main content area is titled 'Cipher Groups' and contains a table of cipher groups. The 'test\_CSGroup' entry is selected. The table has columns for Name and Description. The 'test\_CSGroup' entry is highlighted in blue. The page also includes an 'Add' button, an 'Edit' button, and a 'Delete' button. The page footer shows 'Total 40', '25 Per Page', and 'Page 2 of 2'.

<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

中央の「Add」ボタンをクリックします

## ← Configure Cipher Group

Cipher Group Name

Configured (8)

[Remove All](#)

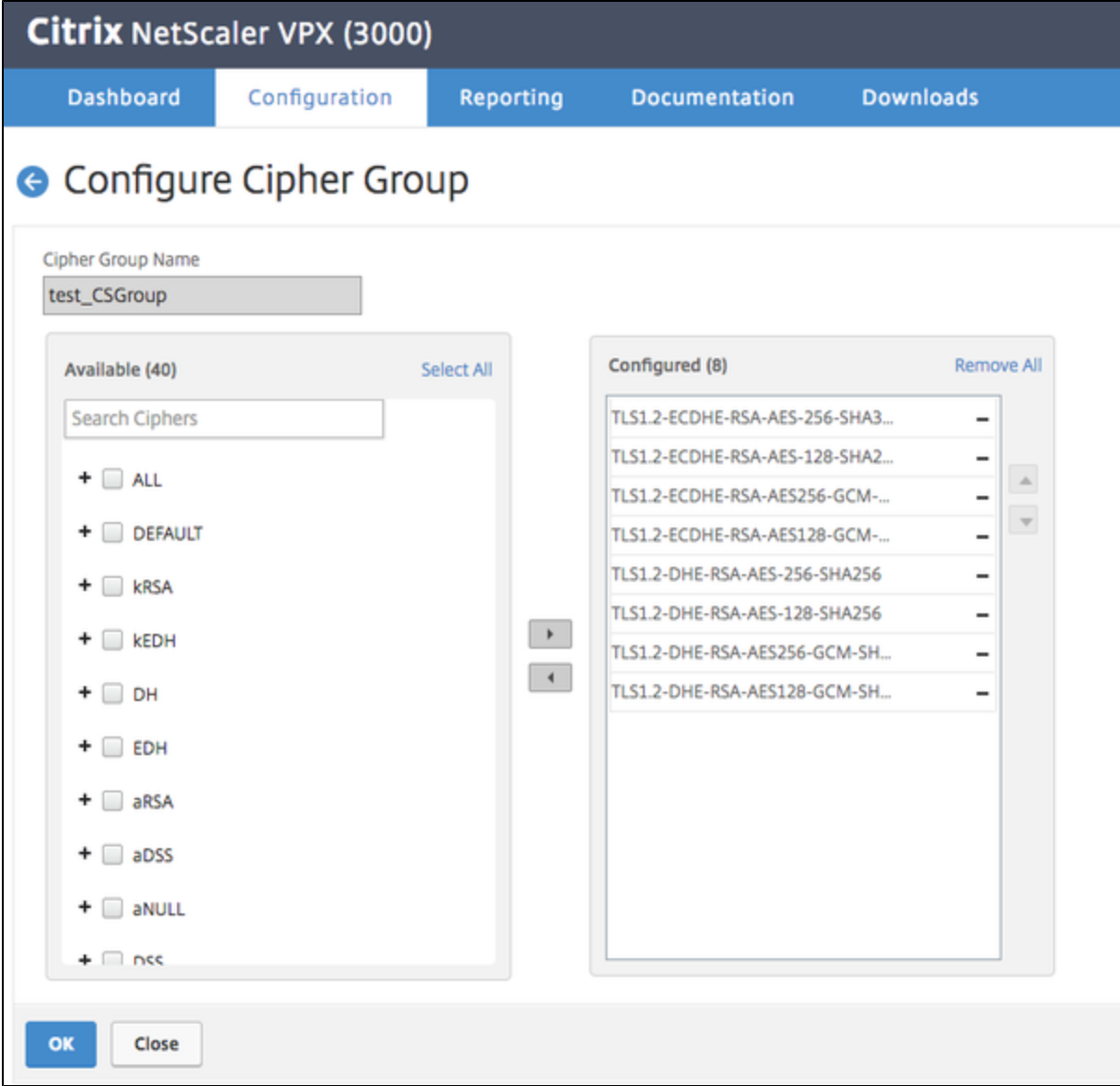
TLS1.2-ECDHE-RSA-AES-256-SHA3...	-
TLS1.2-ECDHE-RSA-AES-128-SHA2...	-
TLS1.2-ECDHE-RSA-AES256-GCM-...	-
TLS1.2-ECDHE-RSA-AES128-GCM-...	-
TLS1.2-DHE-RSA-AES-256-SHA256	-
TLS1.2-DHE-RSA-AES-128-SHA256	-
TLS1.2-DHE-RSA-AES256-GCM-SH...	-
TLS1.2-DHE-RSA-AES128-GCM-SH...	-

[+ Add](#)

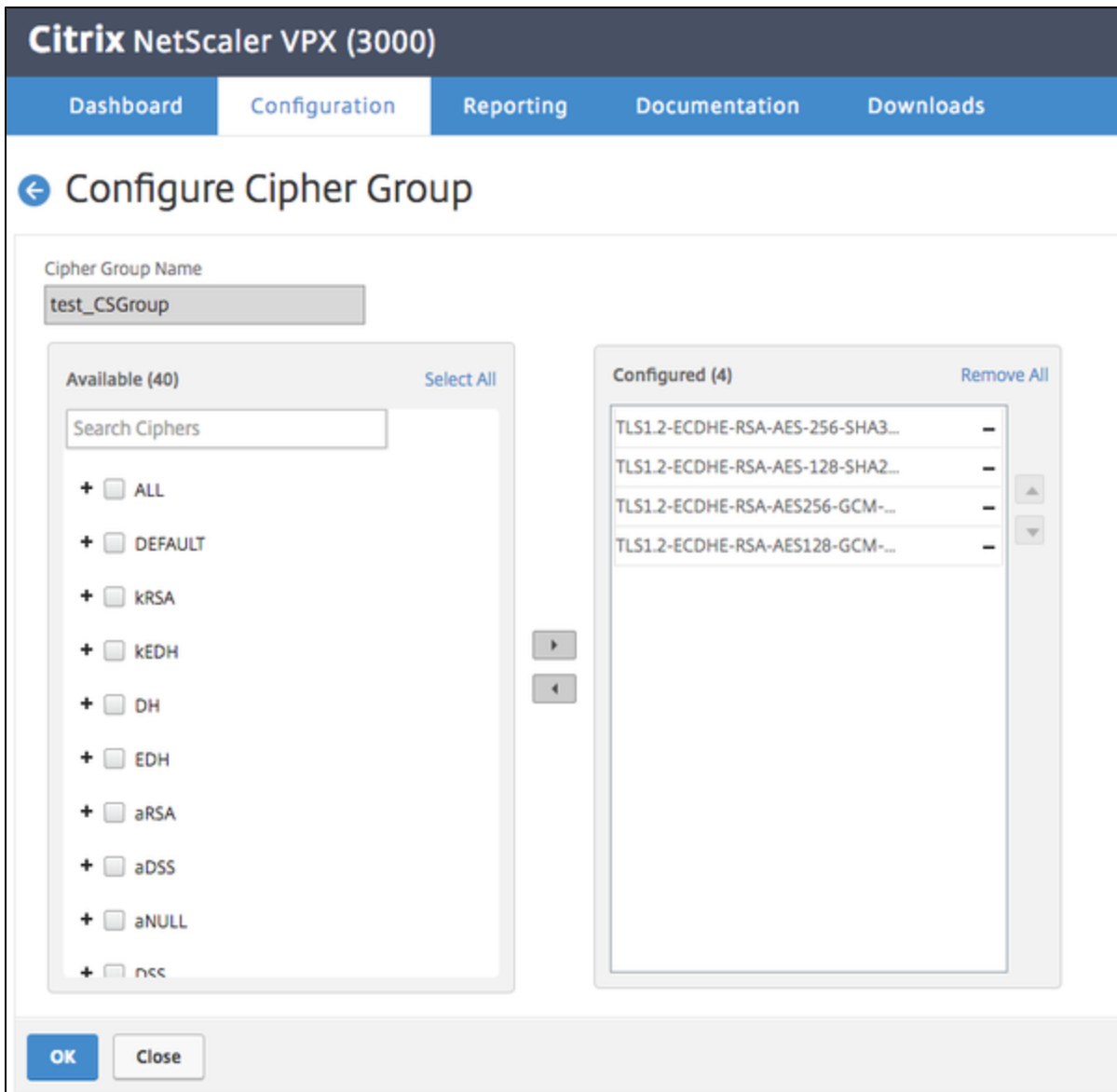
[OK](#)

[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。



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を選択している）



## CLIでの設定方法

realserverに対するクライアント証明書の認証解除

クライアント証明書の認証を利用している場合、serviceのcertkeyNameが設定されています

```
bind ssl service test1 -certkeyName client_cert1
```

以下のコマンドを実行し、クライアント証明書をunbindします

```
> unbind ssl service test1 -certkeyName client_cert1
Done
```

また、クライアント証明書に関しましては、**realserver**におきましても、NetScalerとの接続の際に、クライアント証明書を要求しないように設定ください

## CipherSuiteのDHEを無効化

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

```
DEFAULT
bind ssl service test1 -cipherName DEFAULT

CipherSuite
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
bind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES-256-SHA256
bind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES-128-SHA256
bind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384
bind ssl service test1 -cipherName TLS1.2-DHE-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 service test1 -cipherName DEFAULT
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
bind ssl service test1 -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 service test1 -cipherName TLS1.2-DHE-RSA-AES-256-SHA256
unbind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES-128-SHA256
unbind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384
unbind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES128-GCM-SHA256
```

※DHE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-DHE-RSA-AES-256-SHA256
-cipherPriority 5
bind ssl cipher test_CSGroup -cipherName TLS1.2-DHE-RSA-AES-128-SHA256
-cipherPriority 6
bind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-AES256-GCM-SHA384 -cipherPriority 7
bind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-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-DHE-RSA-AES-256-SHA256
unbind ssl cipher test_CSGroup -cipherName TLS1.2-DHE-RSA-AES-128-SHA256
unbind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-AES256-GCM-SHA384
unbind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-AES128-GCM-SHA256
```