脆弱性(CTX230612)の対応方法

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ChiperSuiteを利用しない

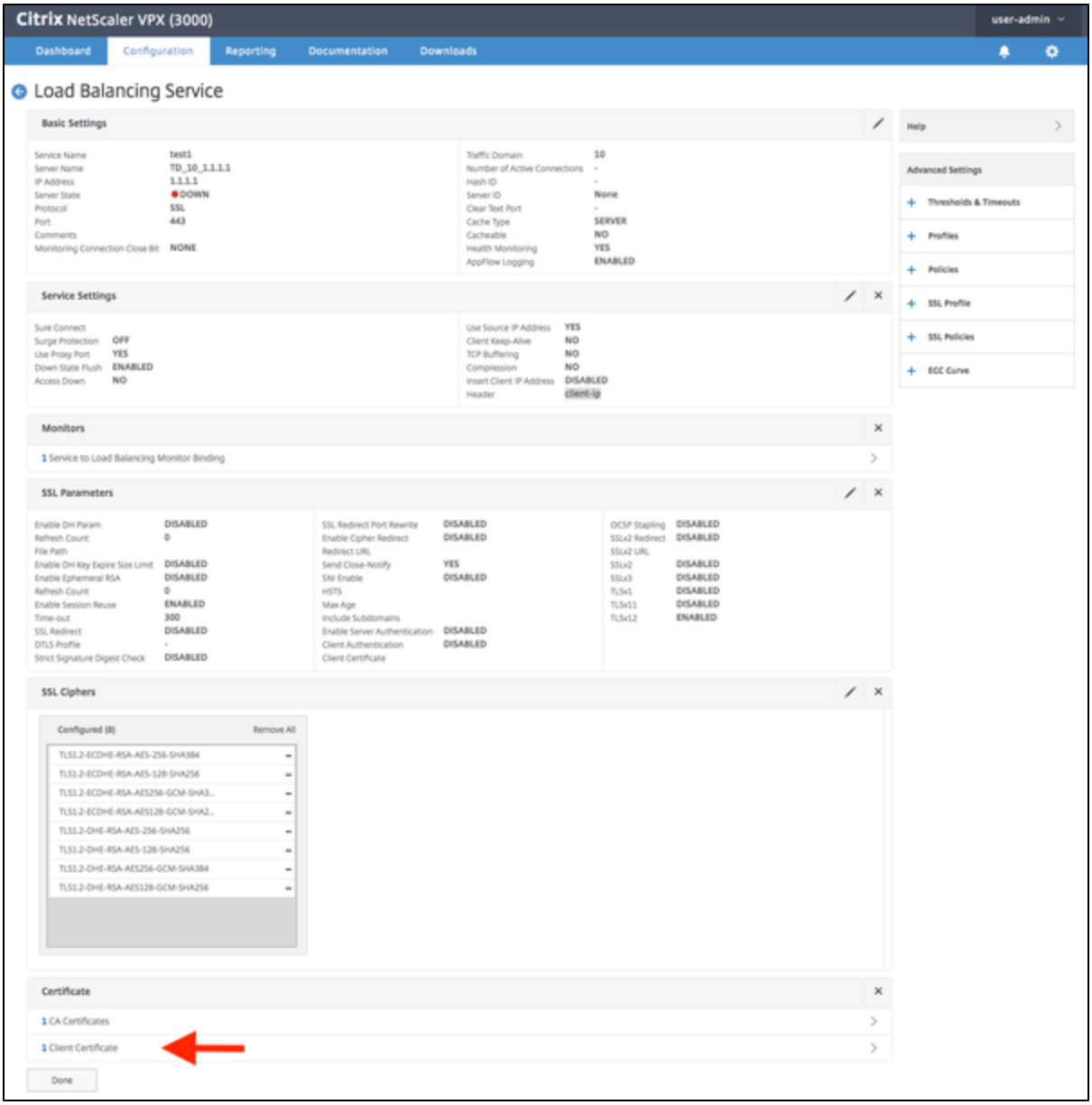
設定手順

GUIでの設定方法

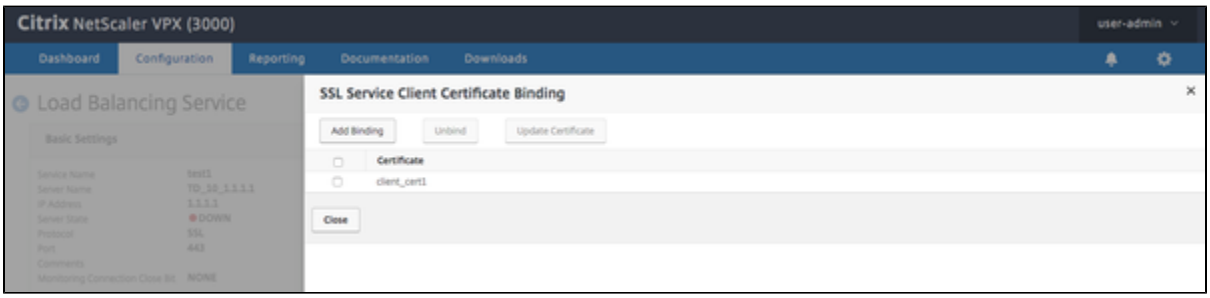
realserverに対するクライアント証明書の認証解除

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。

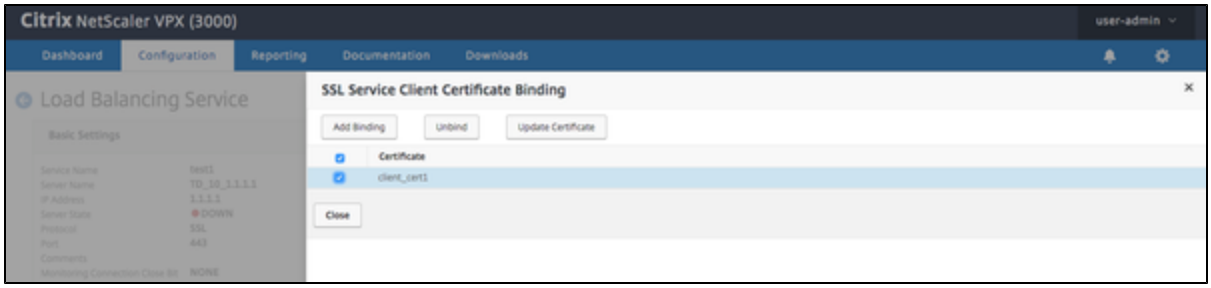
「Traffic Management」-「Load Balancing」-「Services」のLoad Balancing
Service設定画面でclient証明書の認証を利用している場合、certificateにClient証明書が登録されています



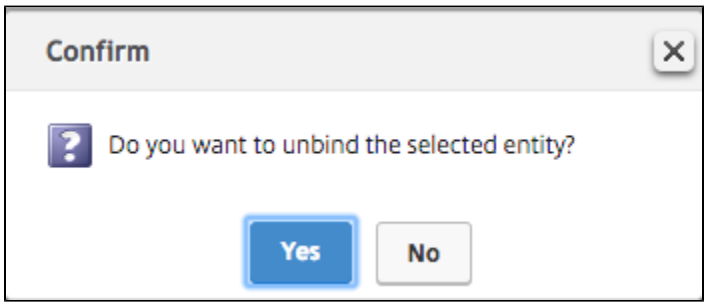
上記のClient Certificateの箇所をクリックすると下図に遷移します



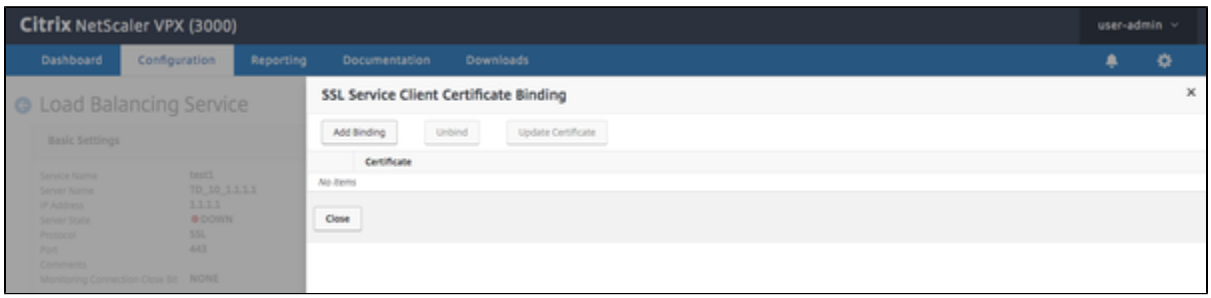
クライアント証明書を選択し、Unbindボタンをクリックします

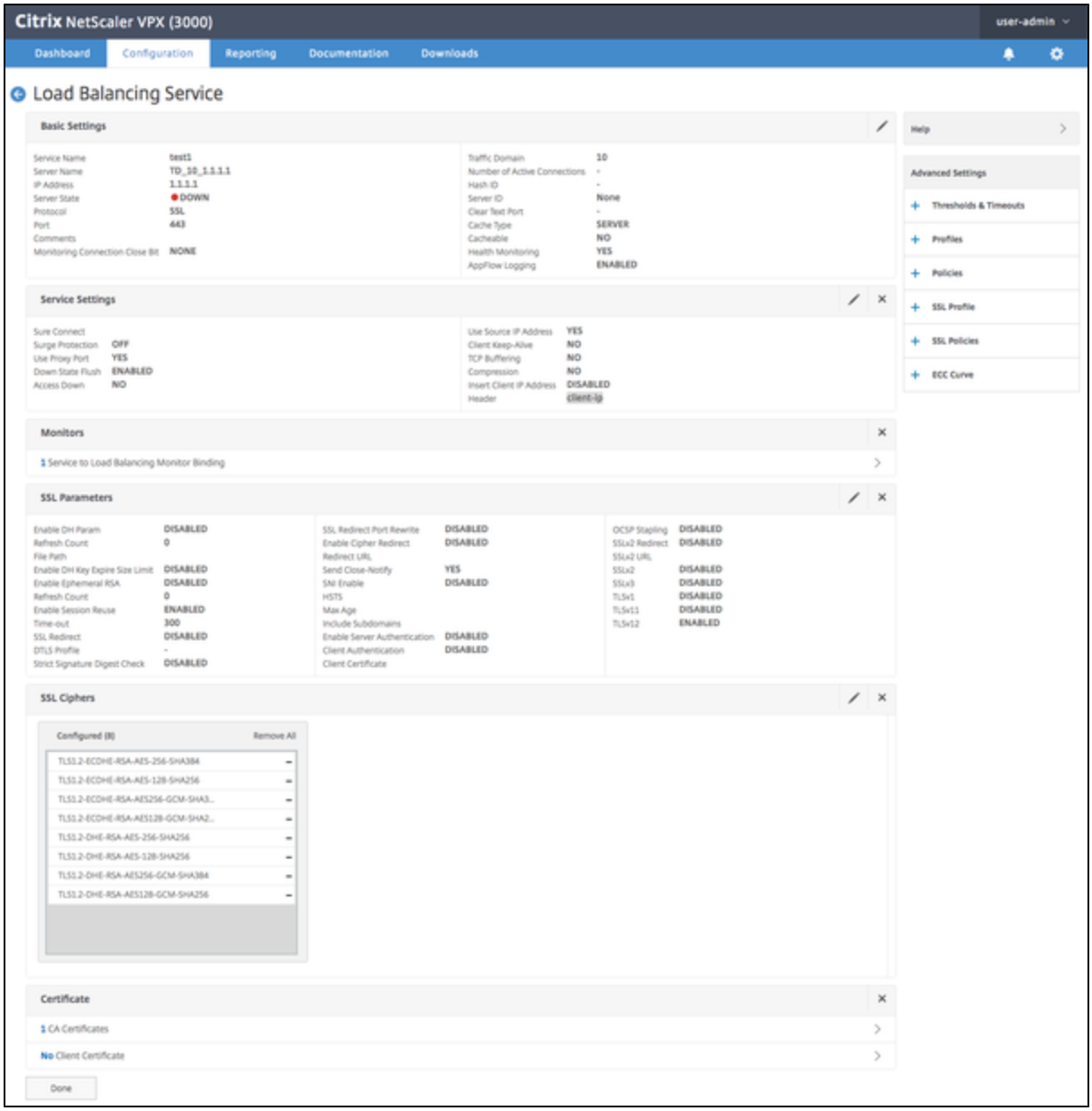


下記メッセージが表示されたらYesを選択します



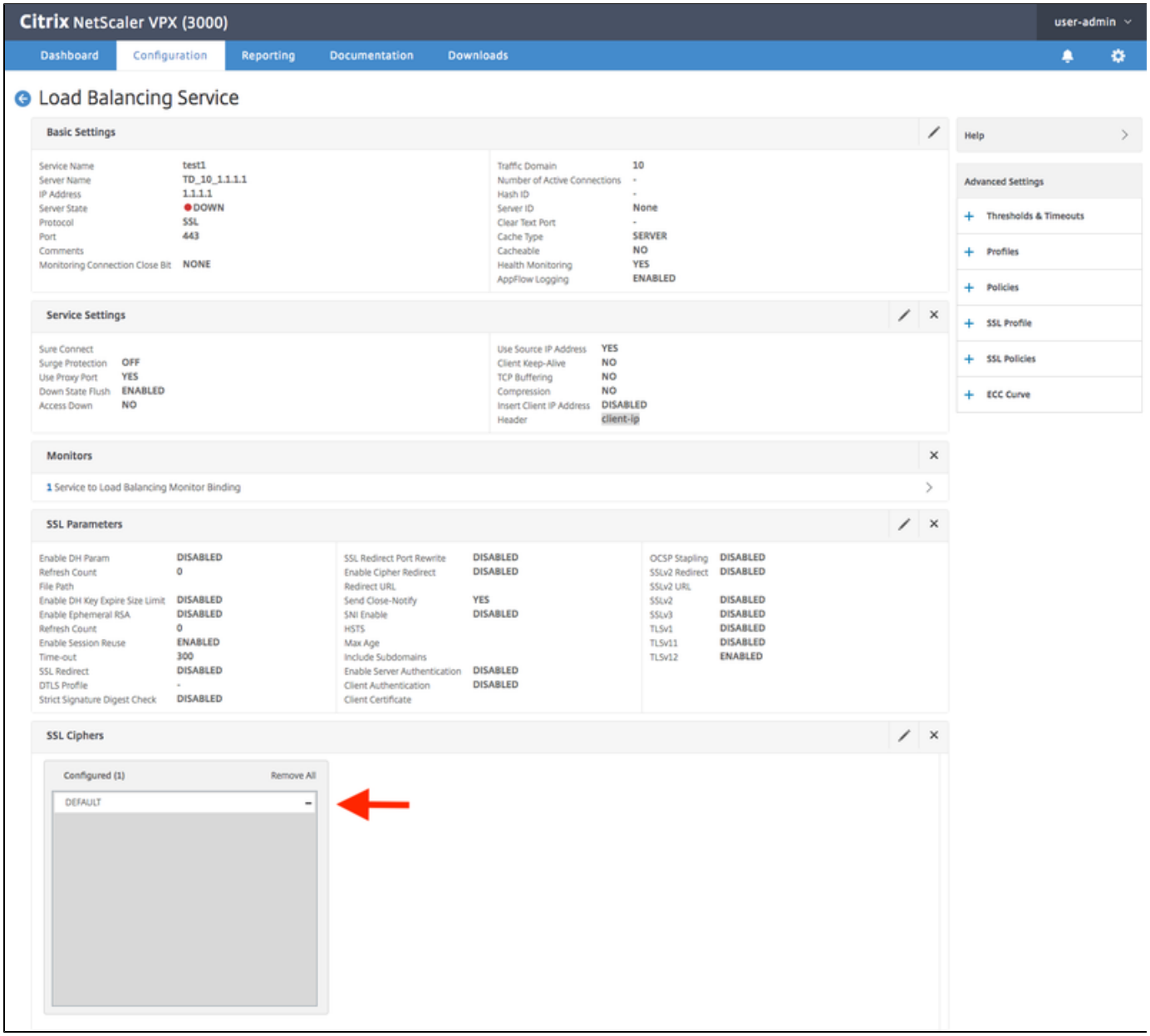
Unbindされていることを確認し、Closeボタンをクリックします

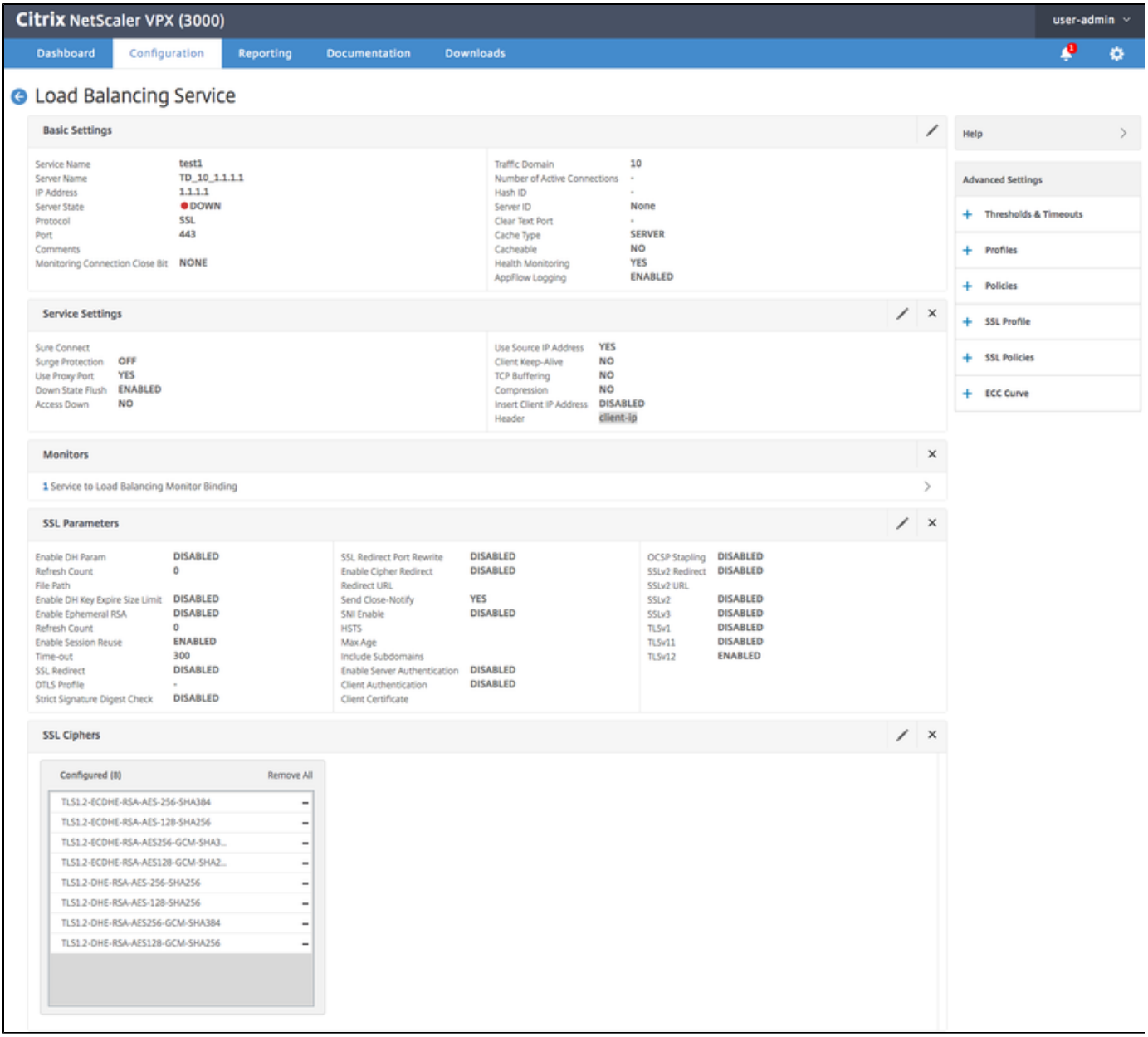




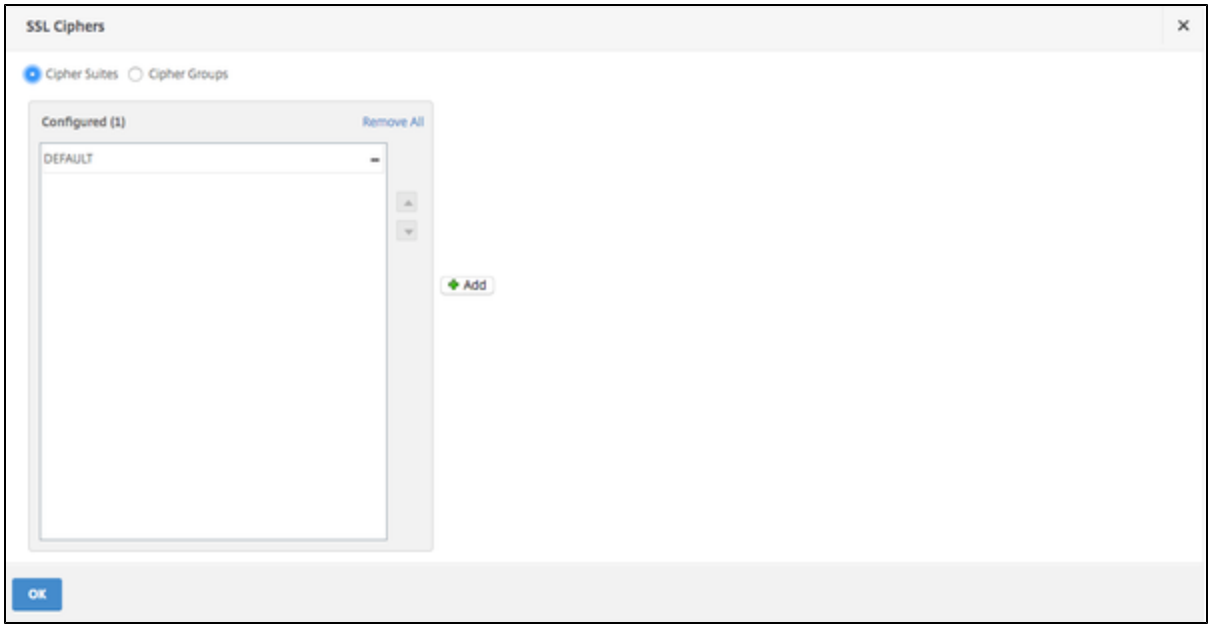
CipherSuiteのDHEを無効化

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


Citrix NetScaler VPX (3000)
user-admin
Dashboard
Configuration
Reporting
Documentation
Downloads
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
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 DISABLED
Header 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
TLSv11 DISABLED
TLSv12 ENABLED
SSL Ciphers
Configured (1)
Remove All
DEFAULT
Help
Advanced Settings
Thresholds & Timeouts
Profiles
Policies
SSL Profile
SSL Policies
ECC Curve

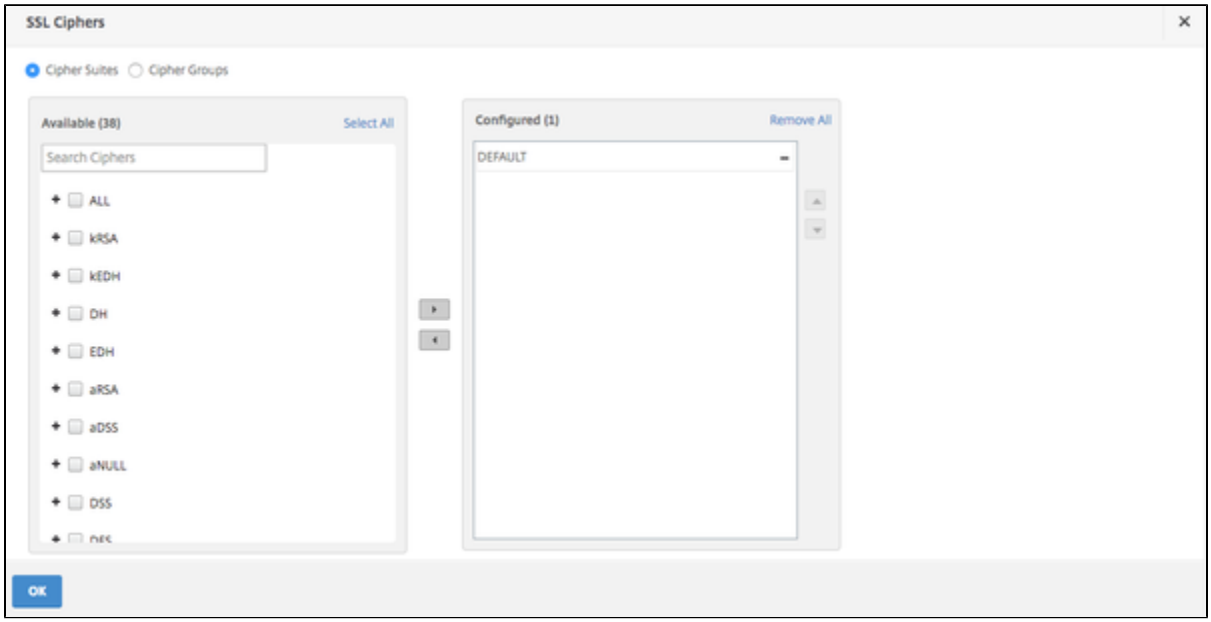


「SSL Ciphers」の編集ボタンをクリックし、中央の「Add」ボタンをクリックします

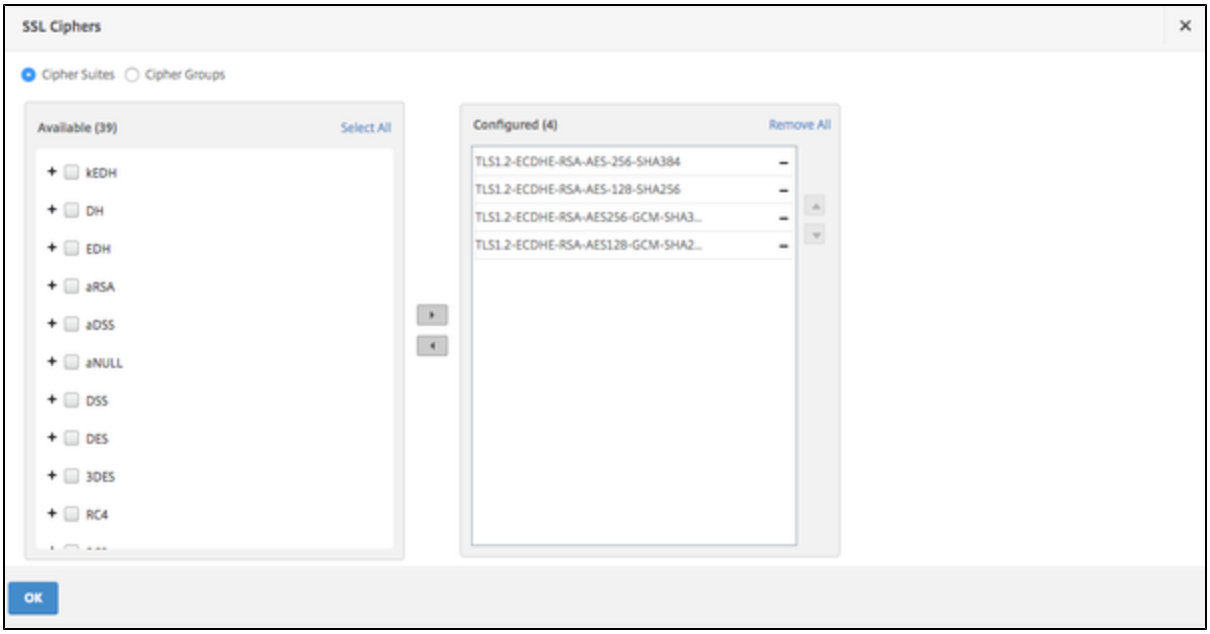


左枠の「Available」から必要なCipherSuiteを選択し、中央にある右向きボタンをクリックして追加します。

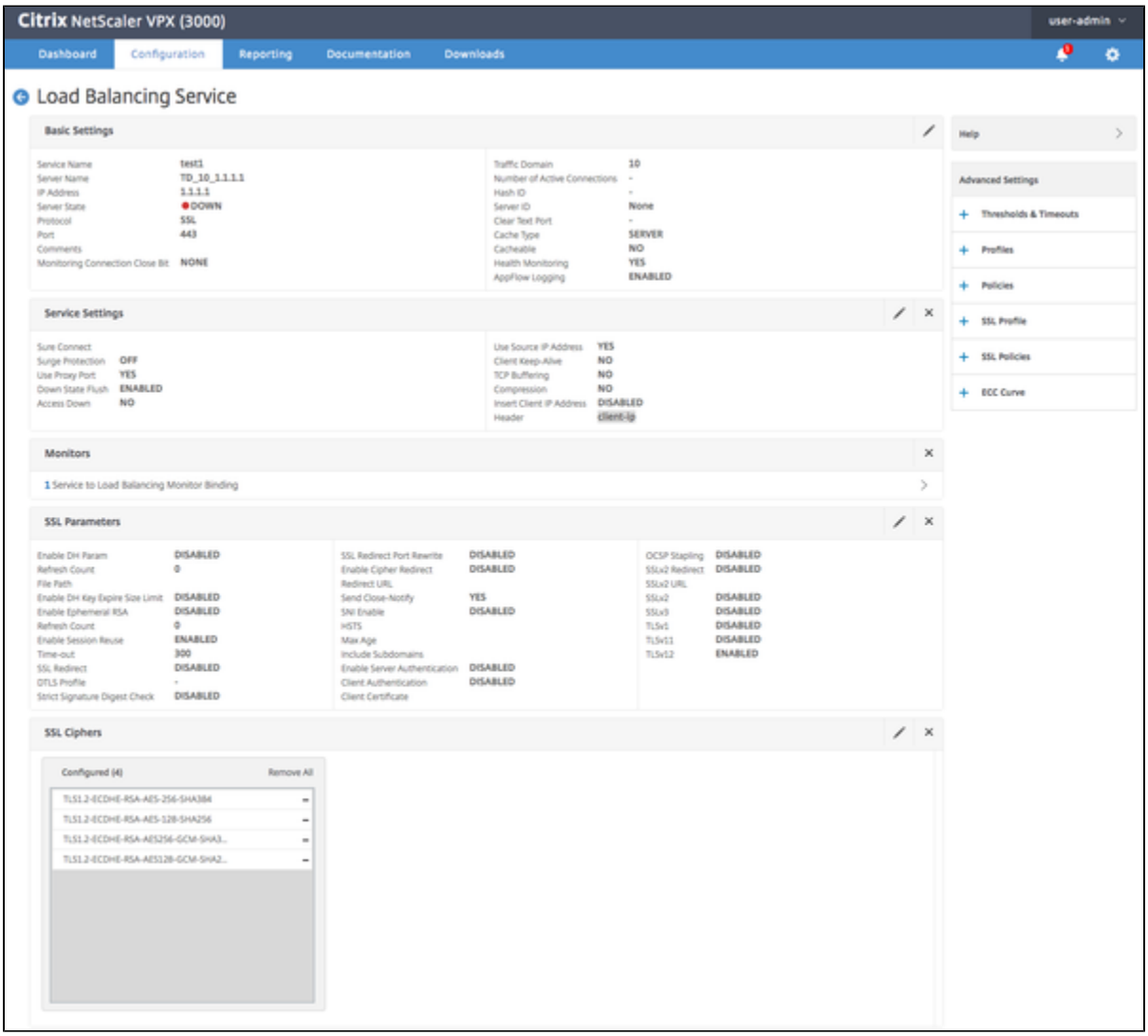
また右枠の「Configured」から、不要なCipherSuiteの右側にある「-」をクリックし削除します。



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）

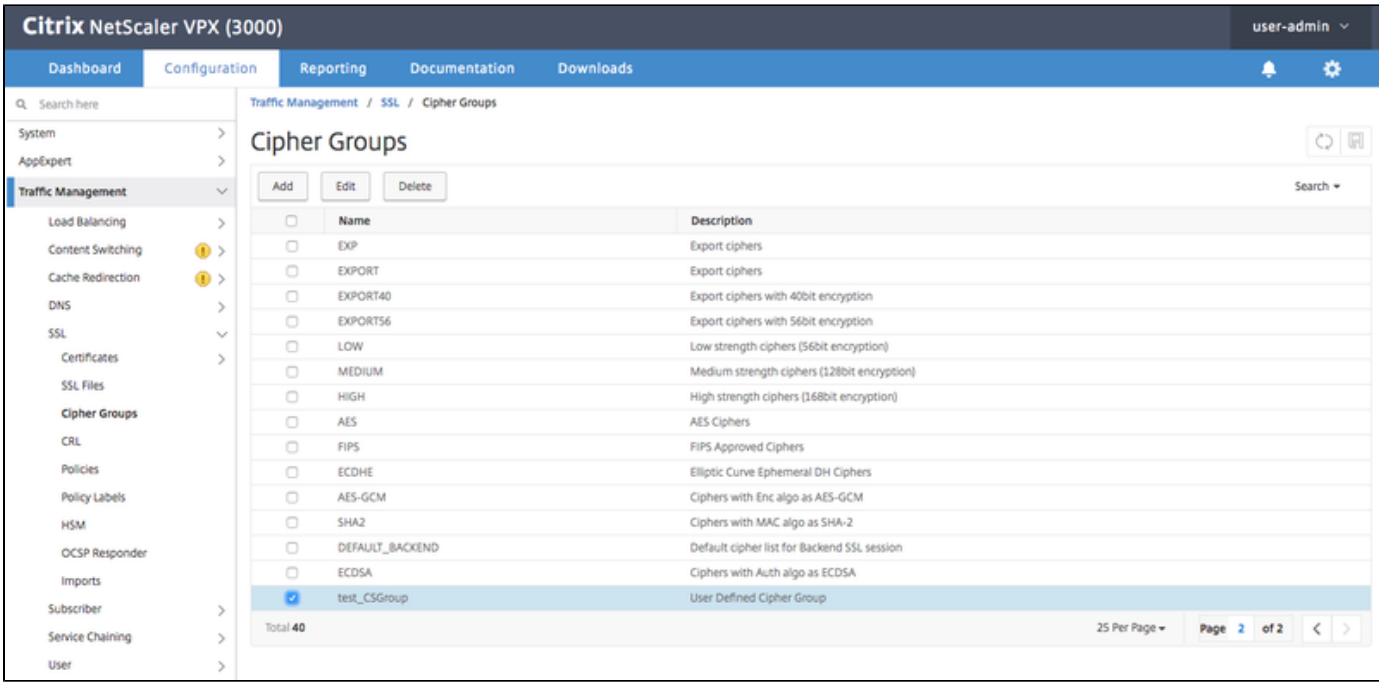


設定が正しく反映されていることを確認し、設定を保存します。

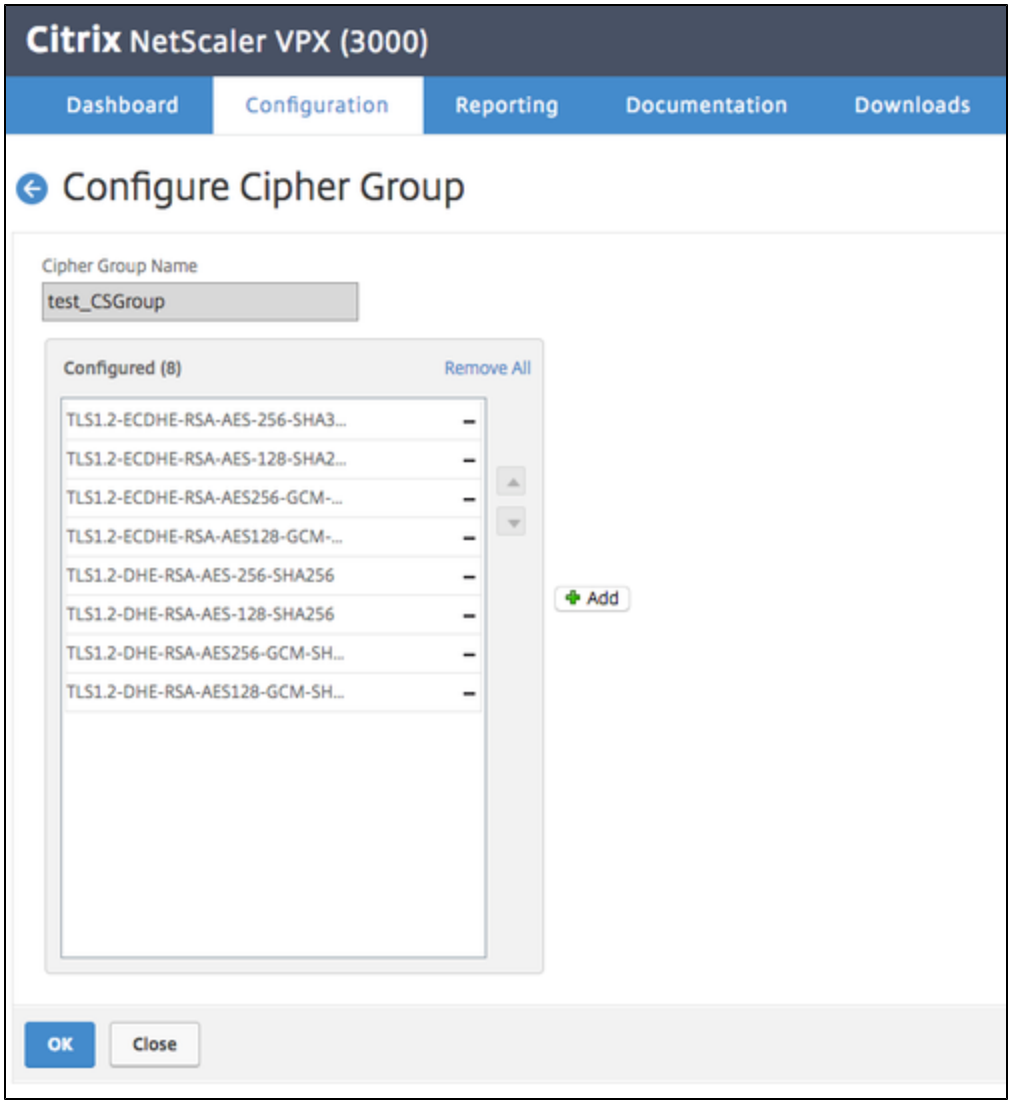


※DHEを含めたCipherGroupを作成して利用している場合は、CipherGroupを編集します（デフォルトのCipher Groupは編集できないため、新たにグループを作成する必要があります）

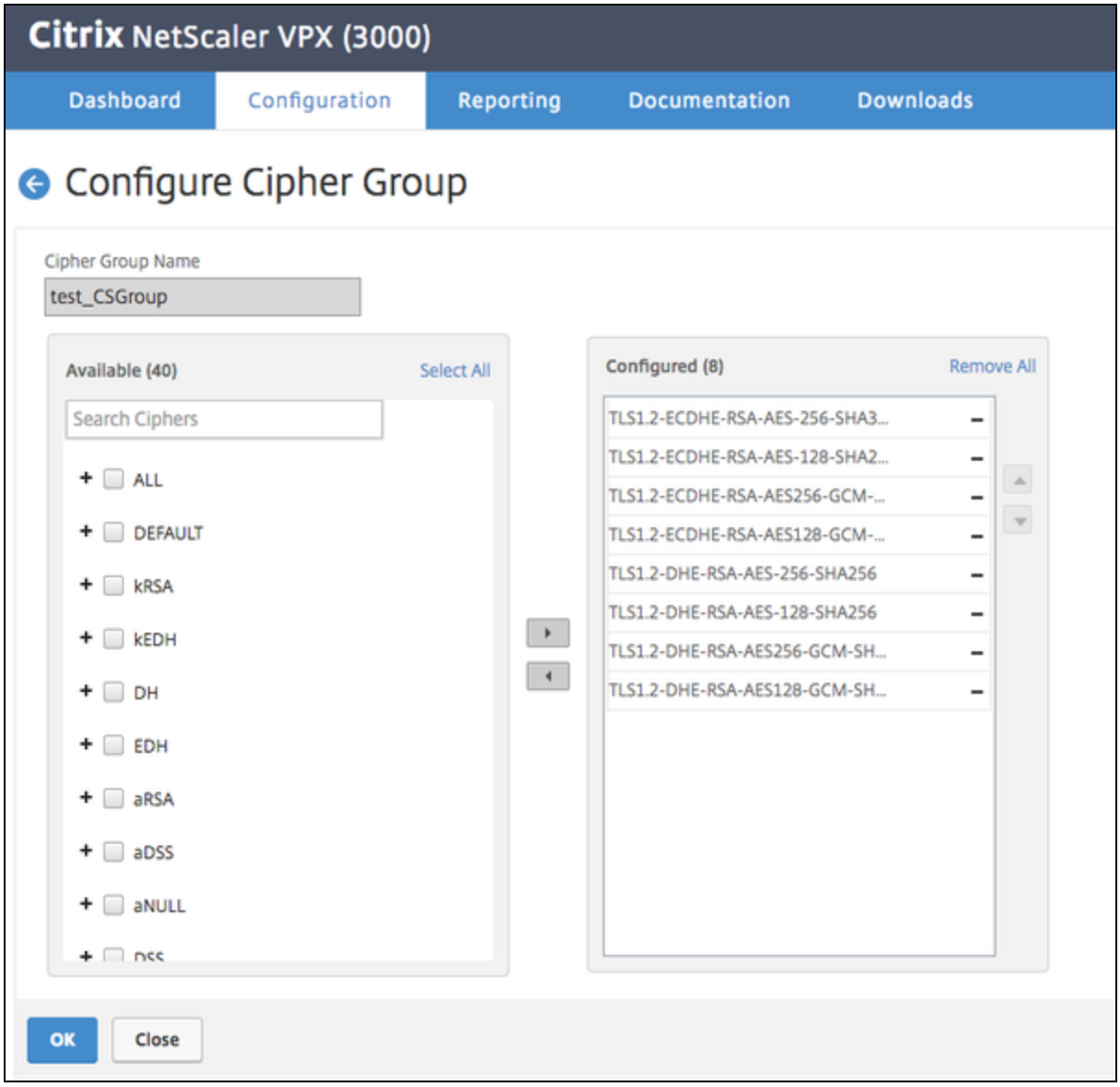
「Traffic Management」-「SSL」-「Ciper Groups」の画面で、利用しているCipher Groupを選択しEditボタンをクリックします。



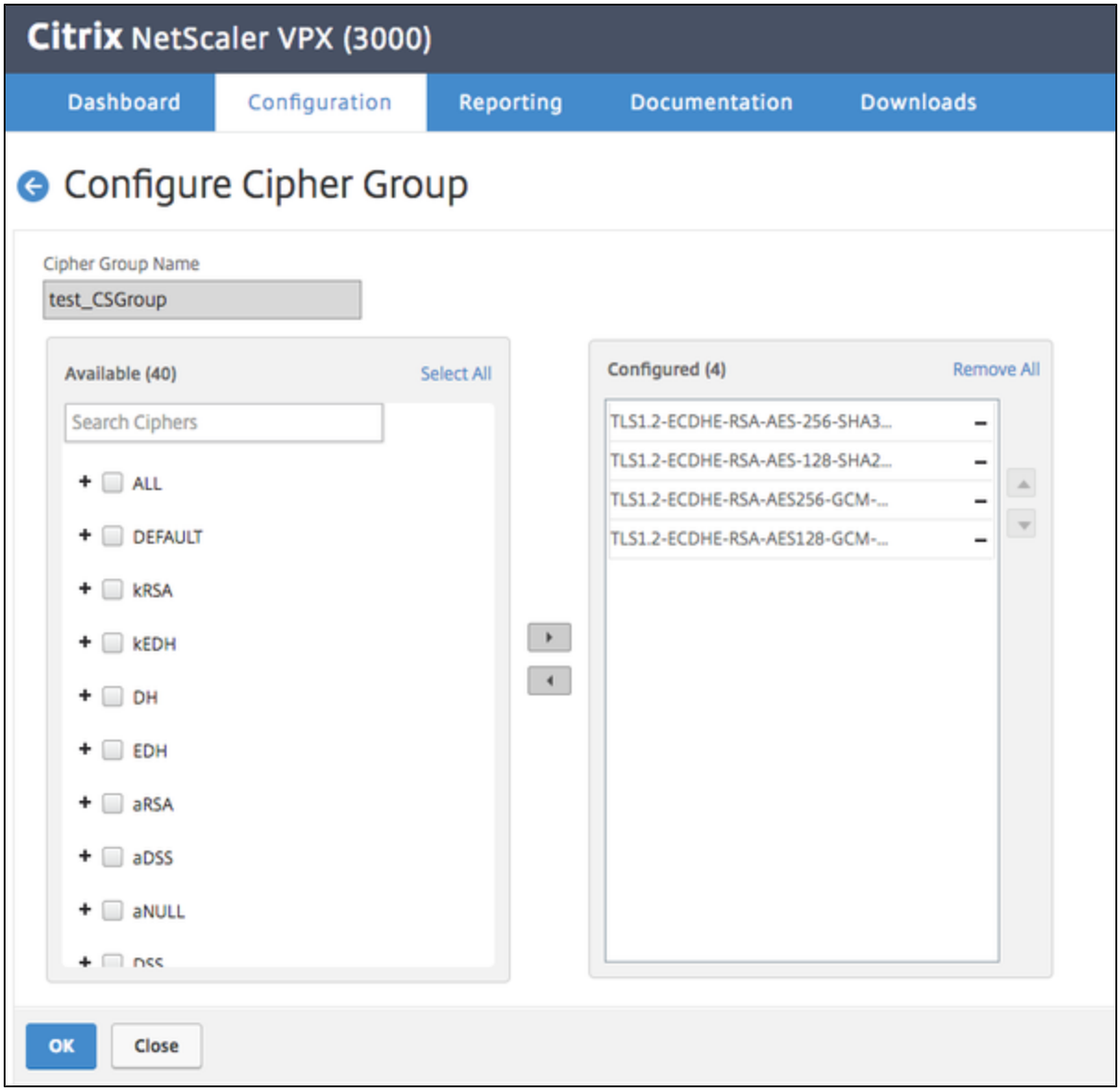
中央の「Add」ボタンをクリックします



右枠の「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
```