脆弱性(CTX234492及びCTX230238)の対応方法

対応方法

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

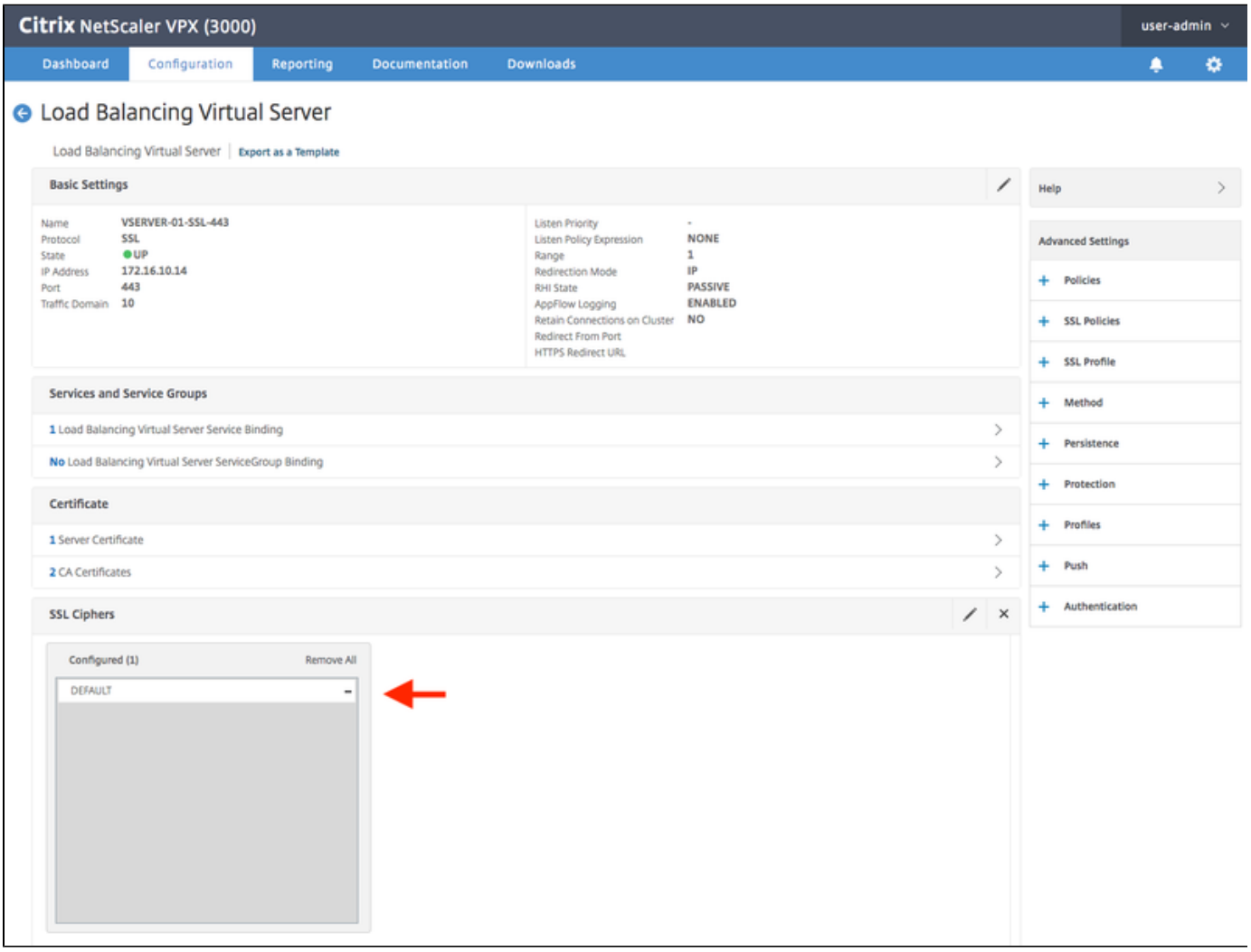
上記を含まないCipherSuiteを使用しないでください。

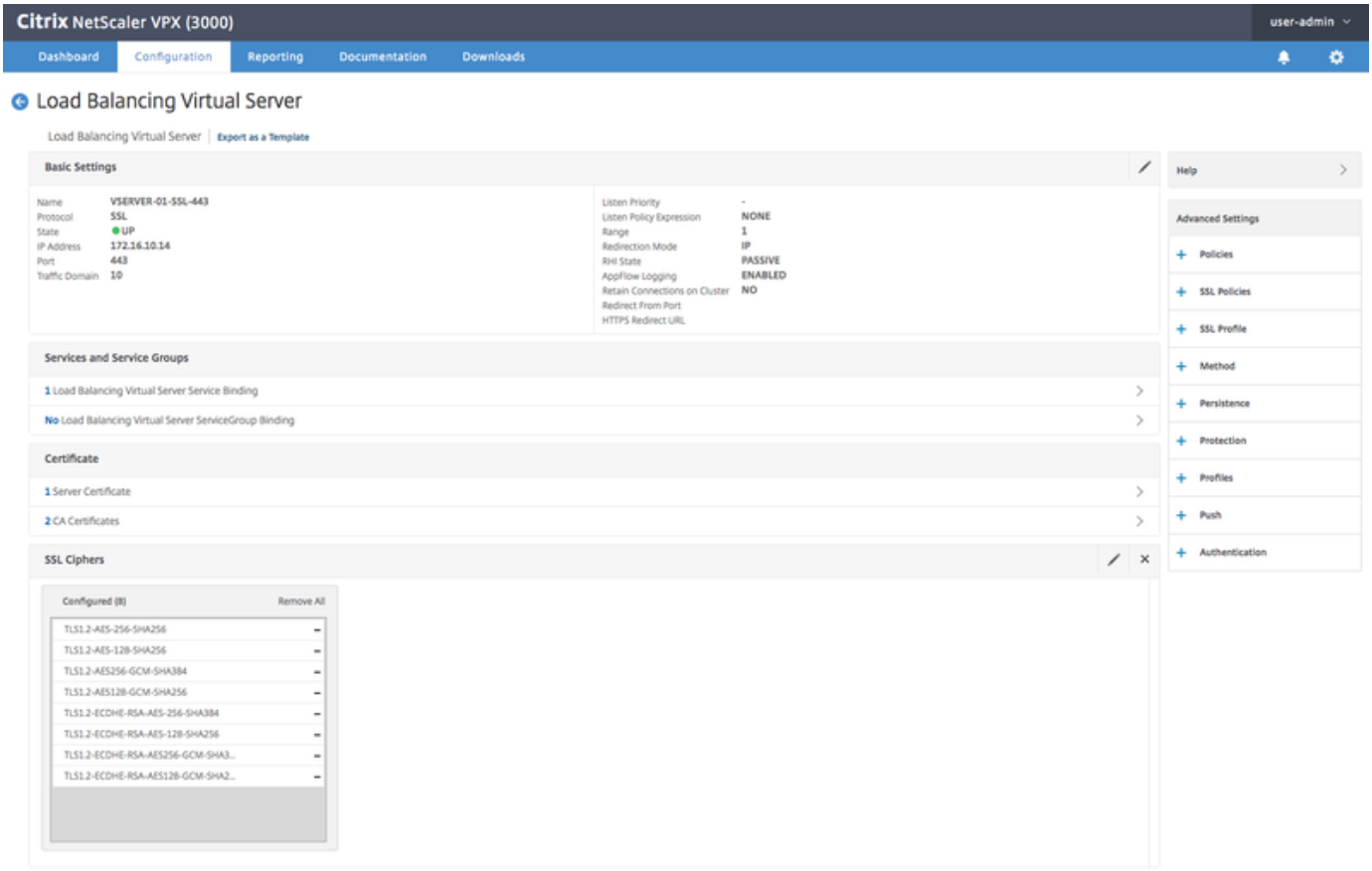
設定手順

GUIでの設定方法

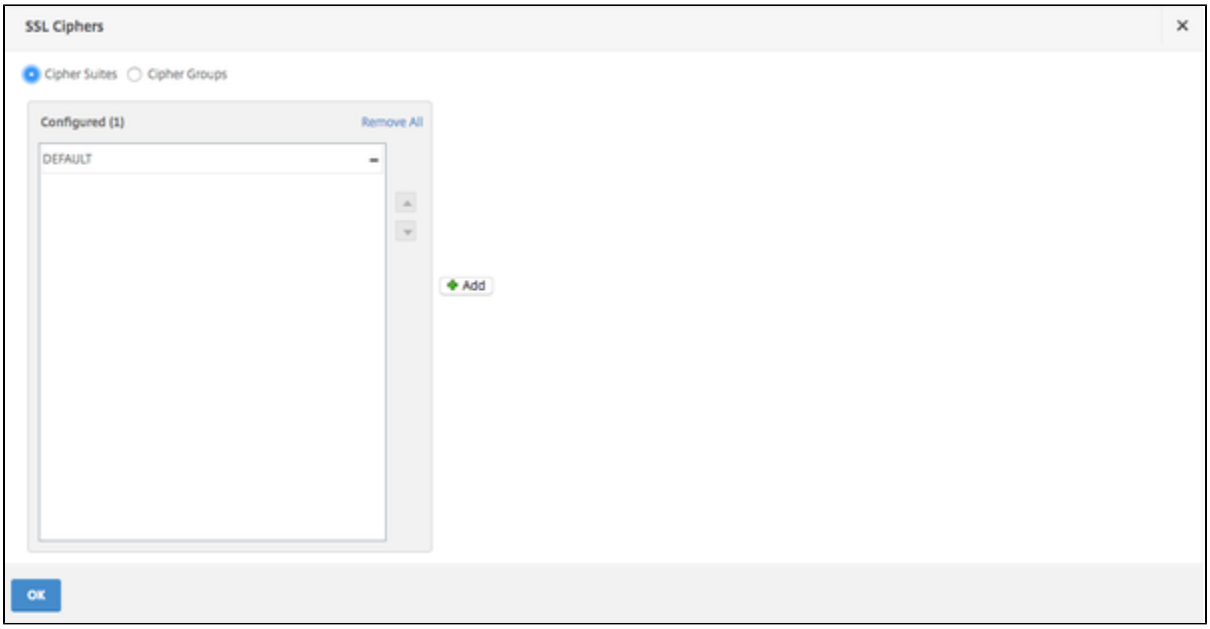
CipherSuiteをPFSに限定

「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



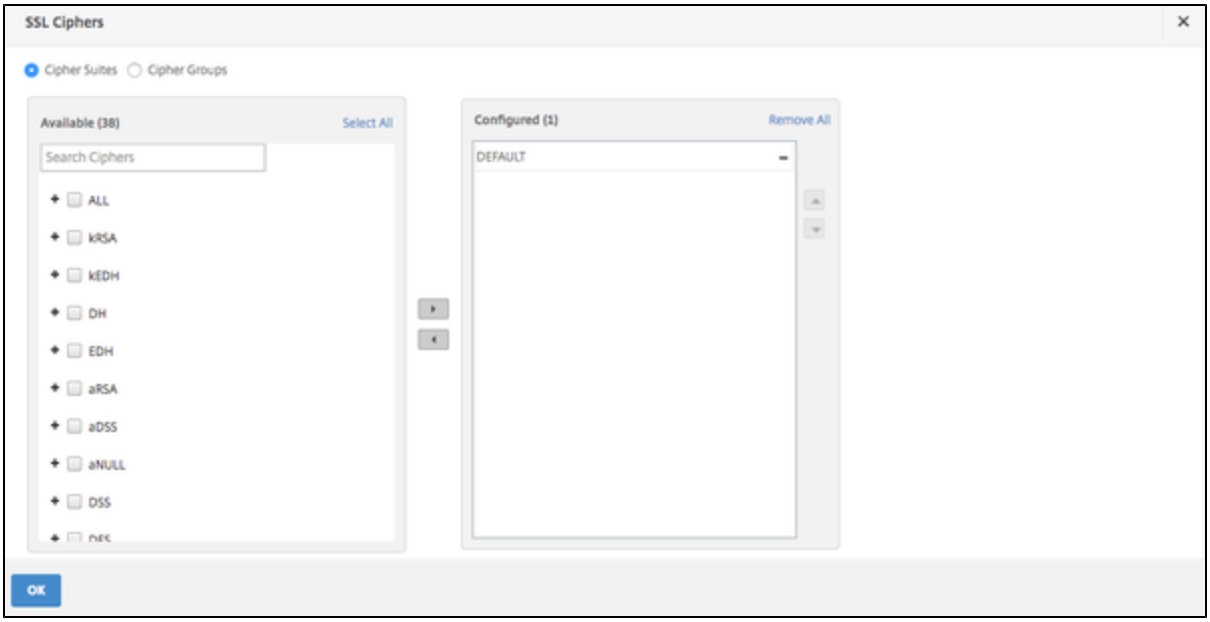


「SSL Ciphers」の編集ボタンをクリックし、中央の「Add」ボタンをクリックします

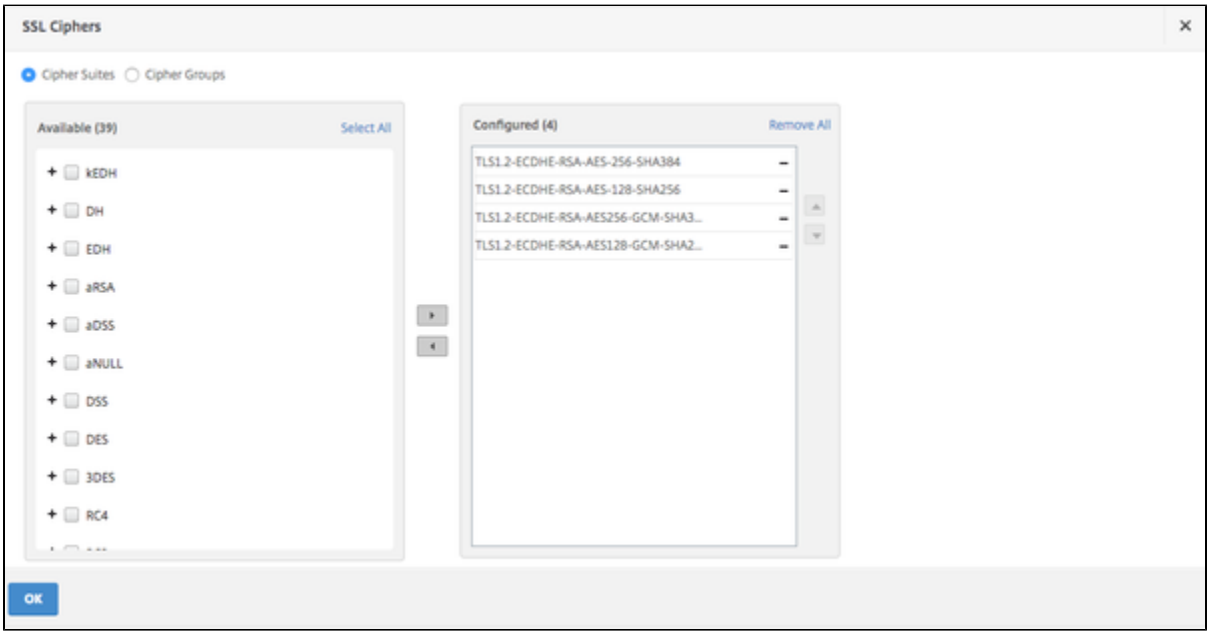


左枠の「Available」から必要なCipherSuiteを選択し、中央にある右向きボタンをクリックして追加します。

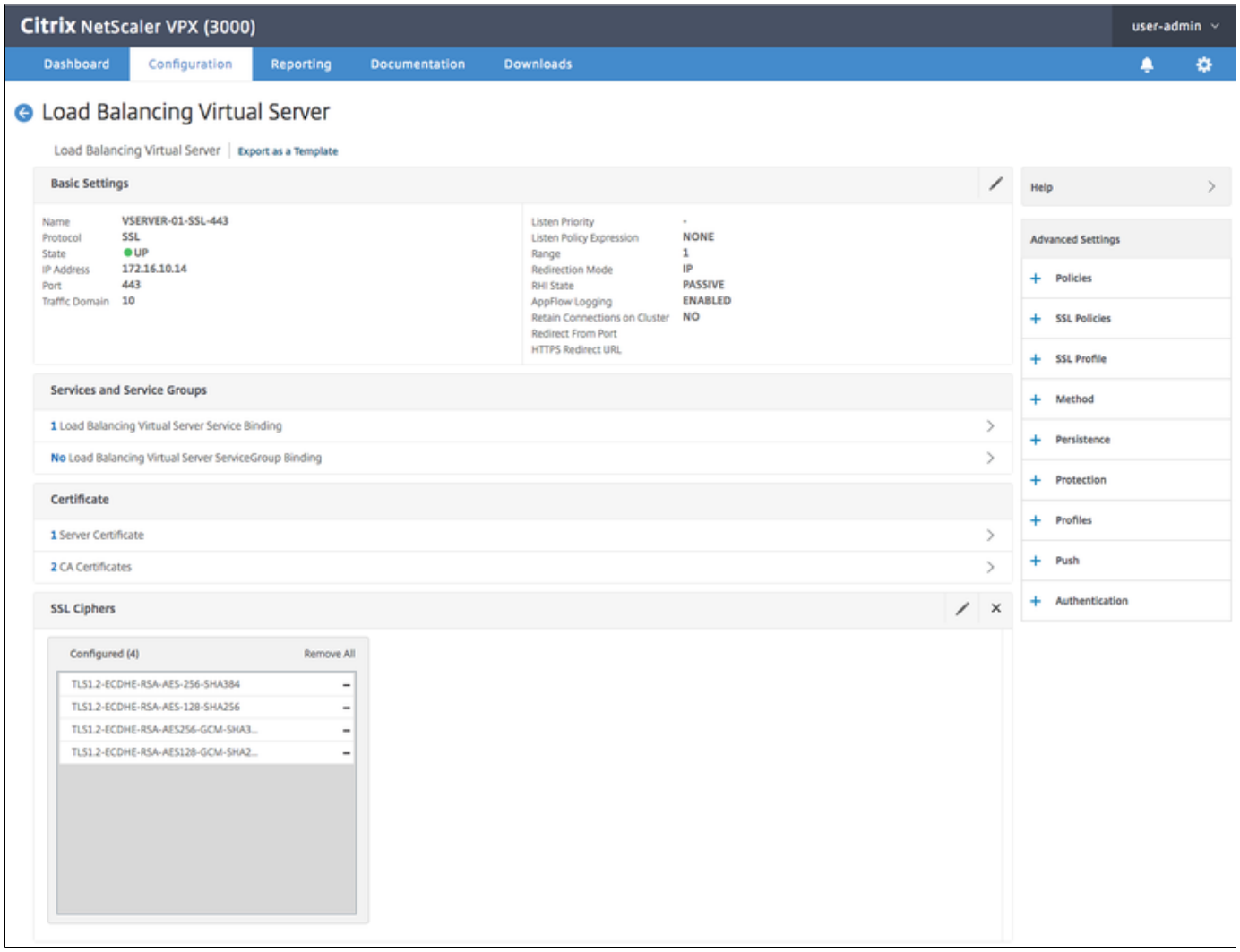
また右枠の「Configured」から、不要なCipherSuiteの右側にある「-」をクリックし削除します。



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）

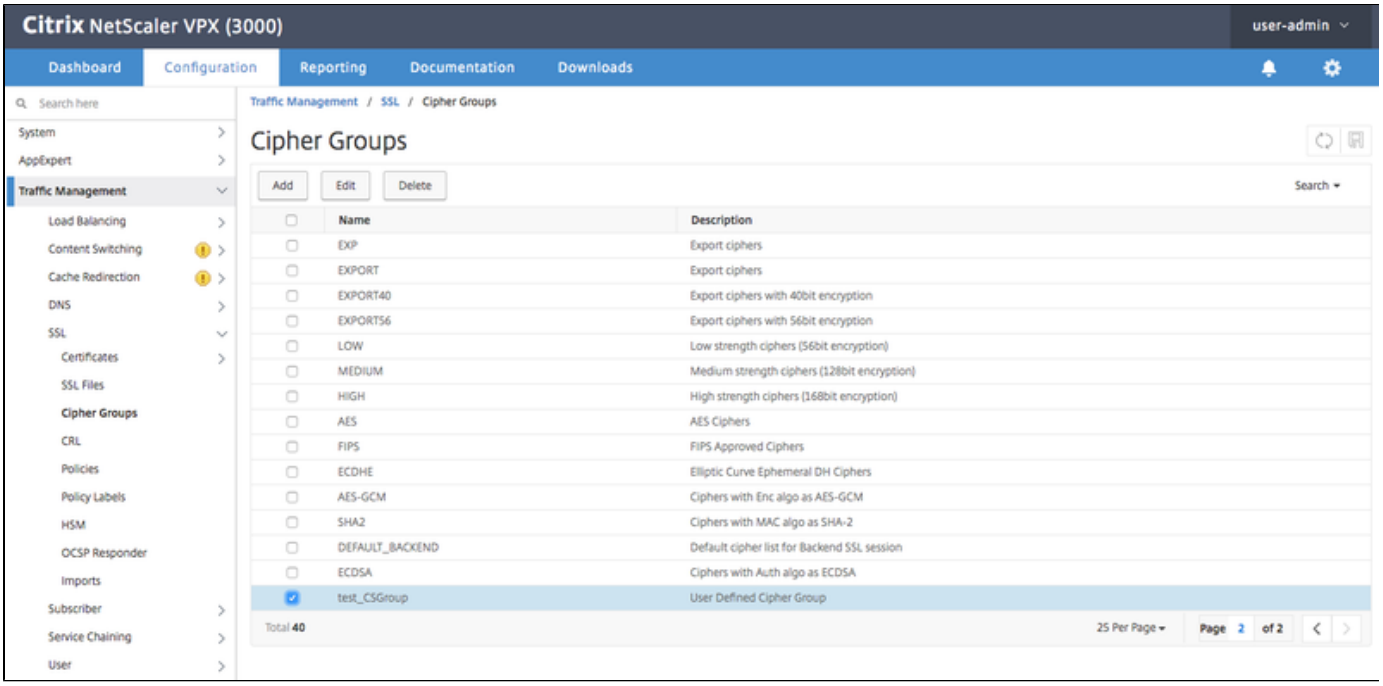


設定が正しく反映されていることを確認し、設定を保存します。

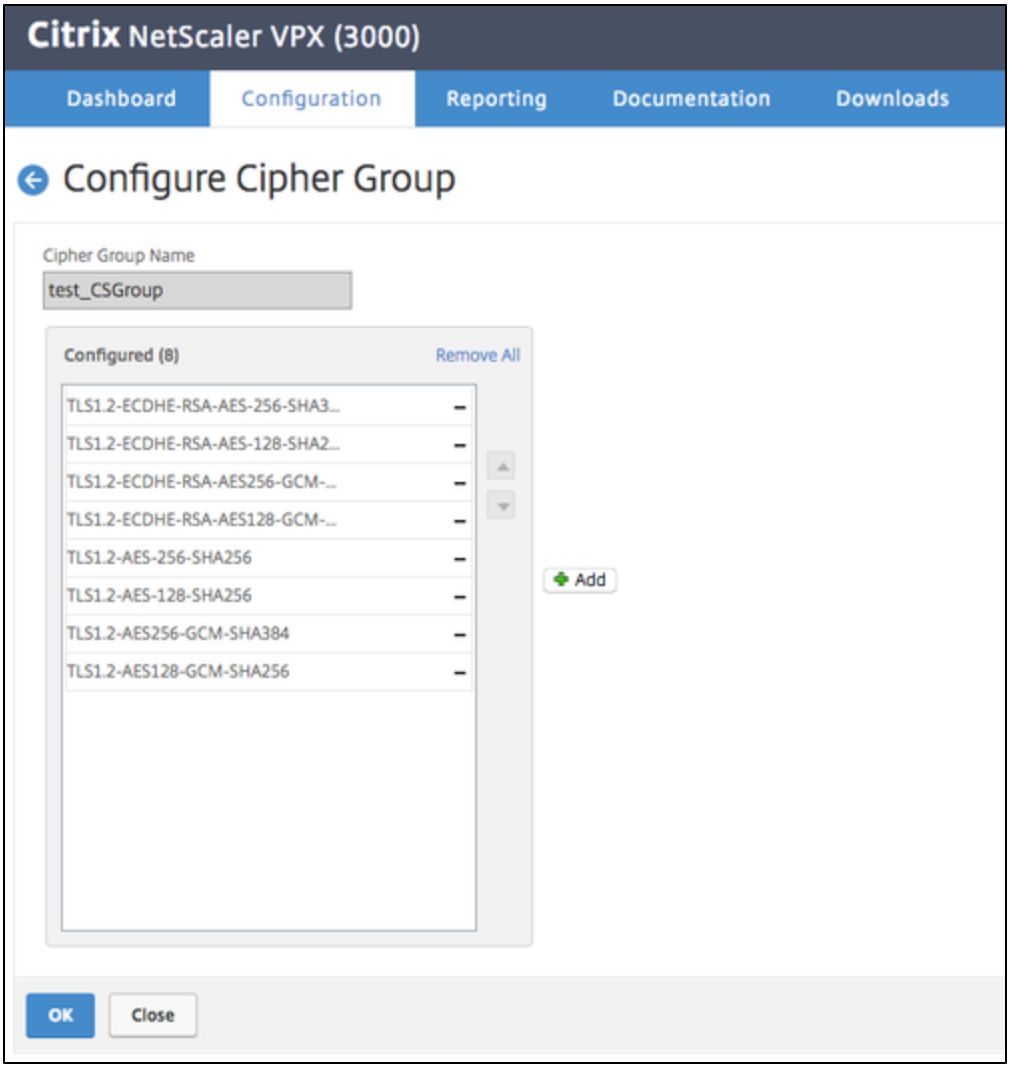


※DHE/ECDHE以外のCipherSuiteを含めたCipherGroupを作成して利用している場合は、CipherGroupを編集します（デフォルトのCipher Groupは編集できないため、新たにグループを作成する必要があります）

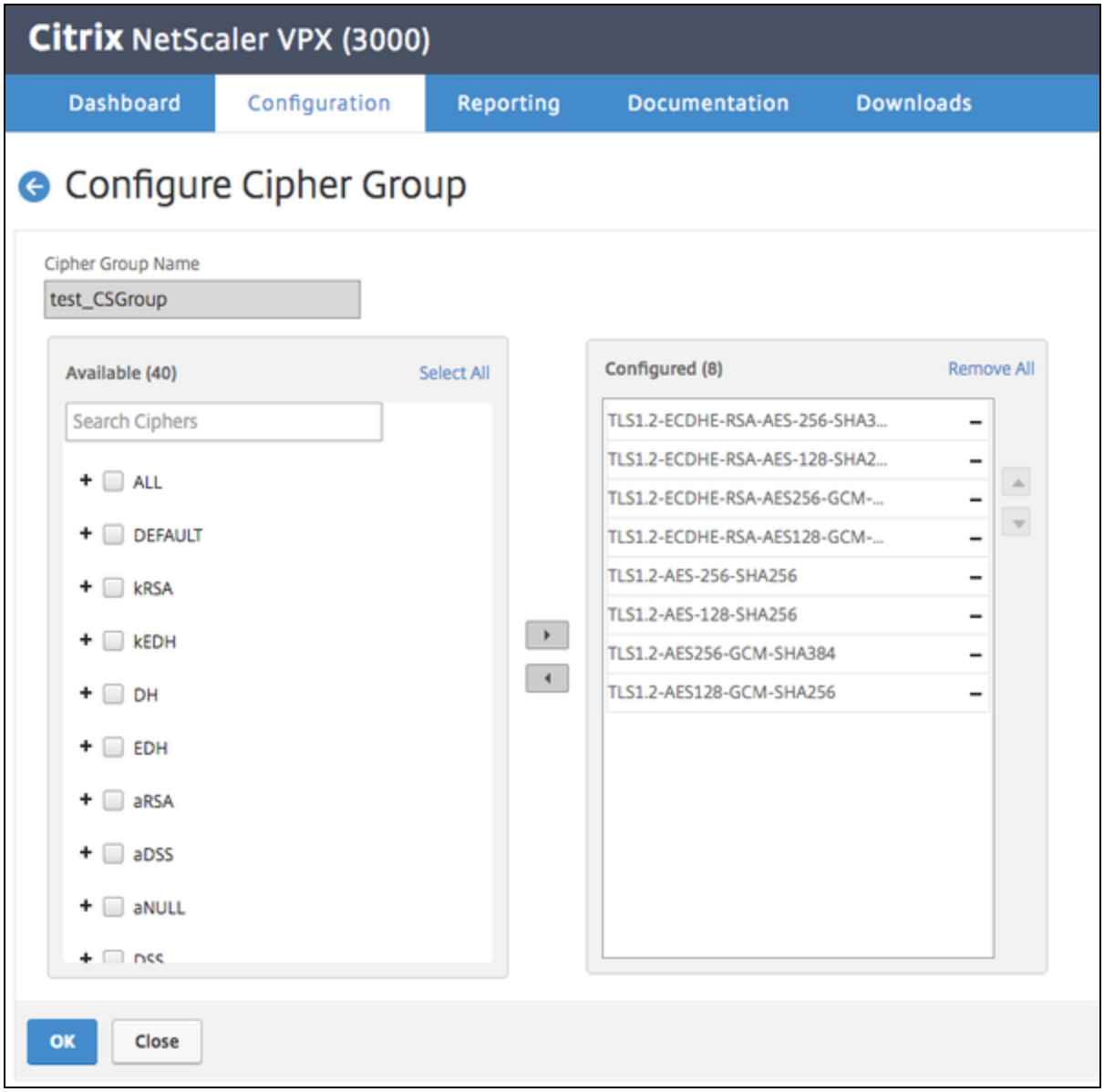
「Traffic Management」-「SSL」-「Cipher Groups」の画面で、利用しているCipher Groupを選択しEditボタンをクリックします。



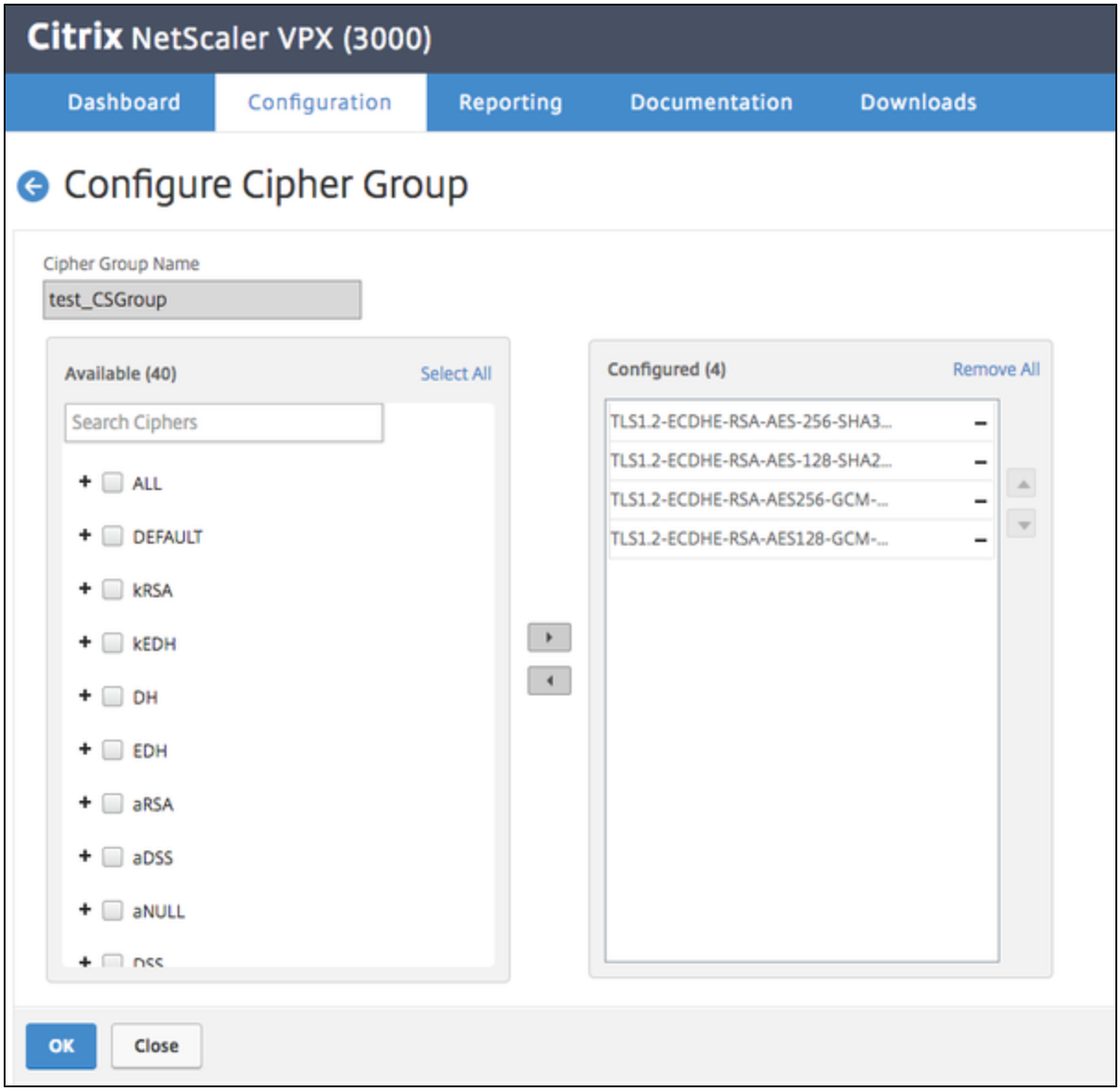
中央の「Add」ボタンをクリックします



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
```