Countermeasures for vulnerability (CTX234492/CTX230238)

- Countermeasures
- Setting method
  - Setting method via GUI
    - Limit the CipherSuite to be used to PFS (DHE / ECDHE)
  - Setting method via CLI
    - Limit the CipherSuite to be used to PFS (DHE / ECDHE)

Countermeasures

Please limit Cipher Suite to be used to PFS (DHE / ECDHE).

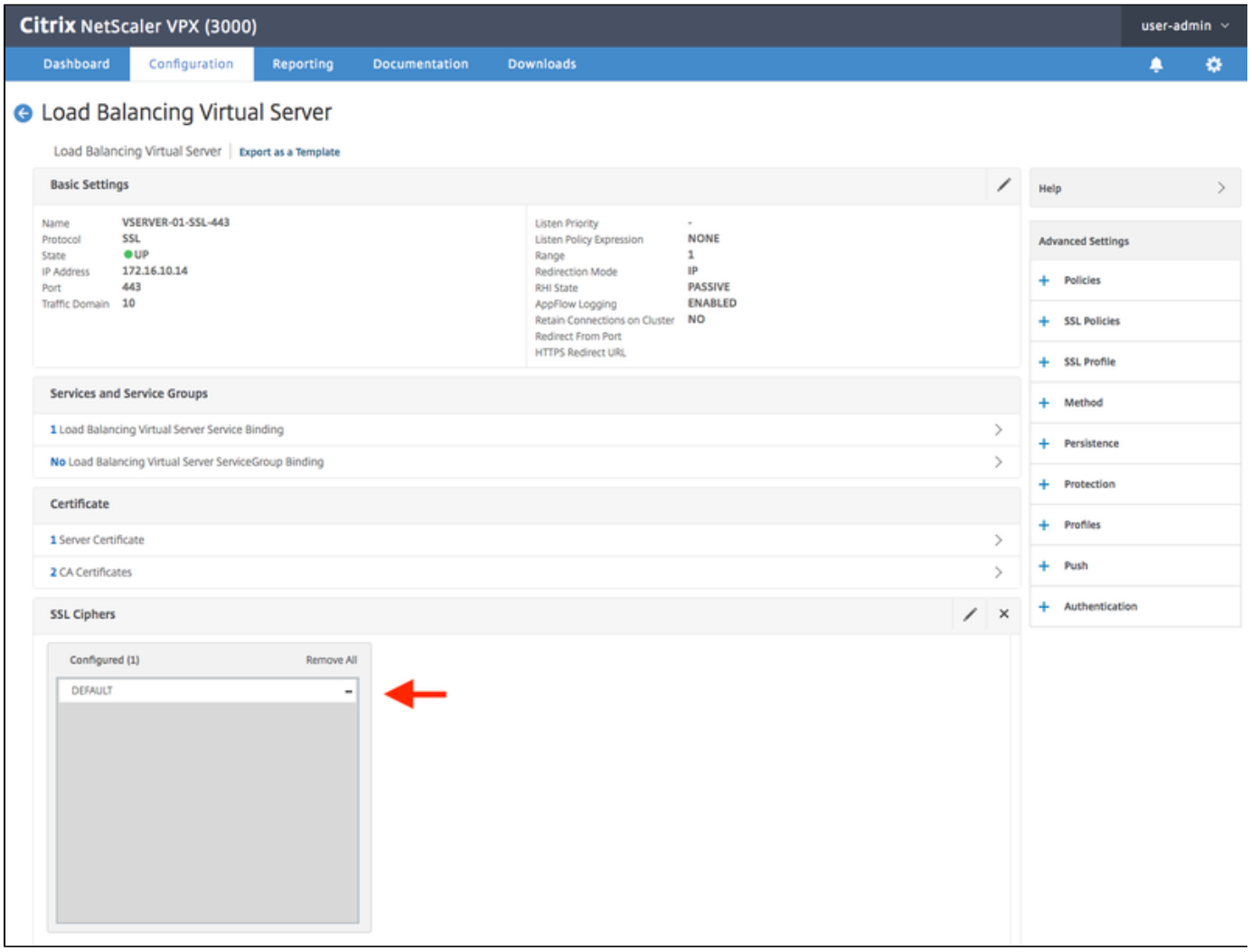
Do not use Cipher Suite which does not includePFS (DHE / ECDHE).

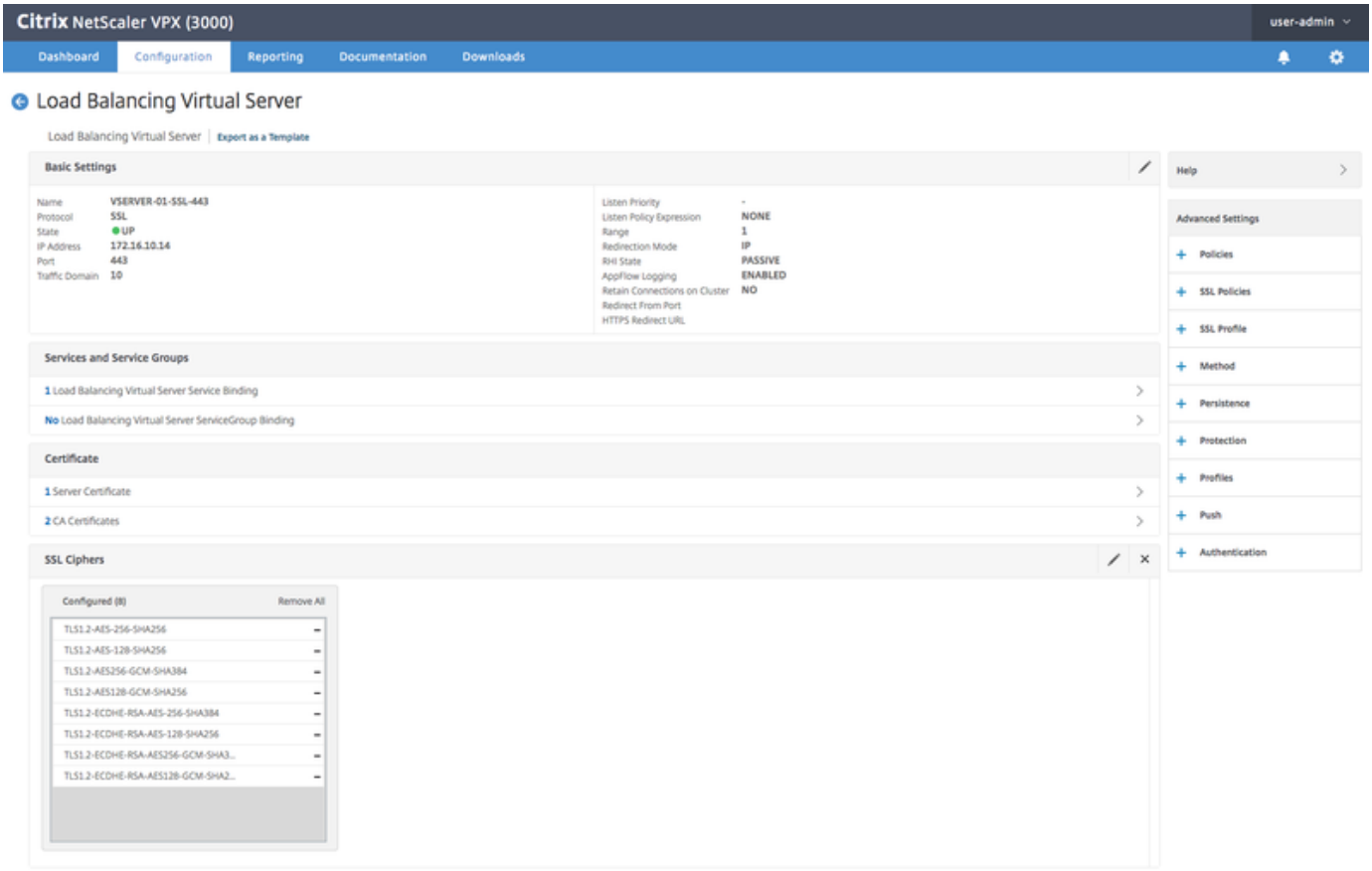
Setting method

Setting method via GUI

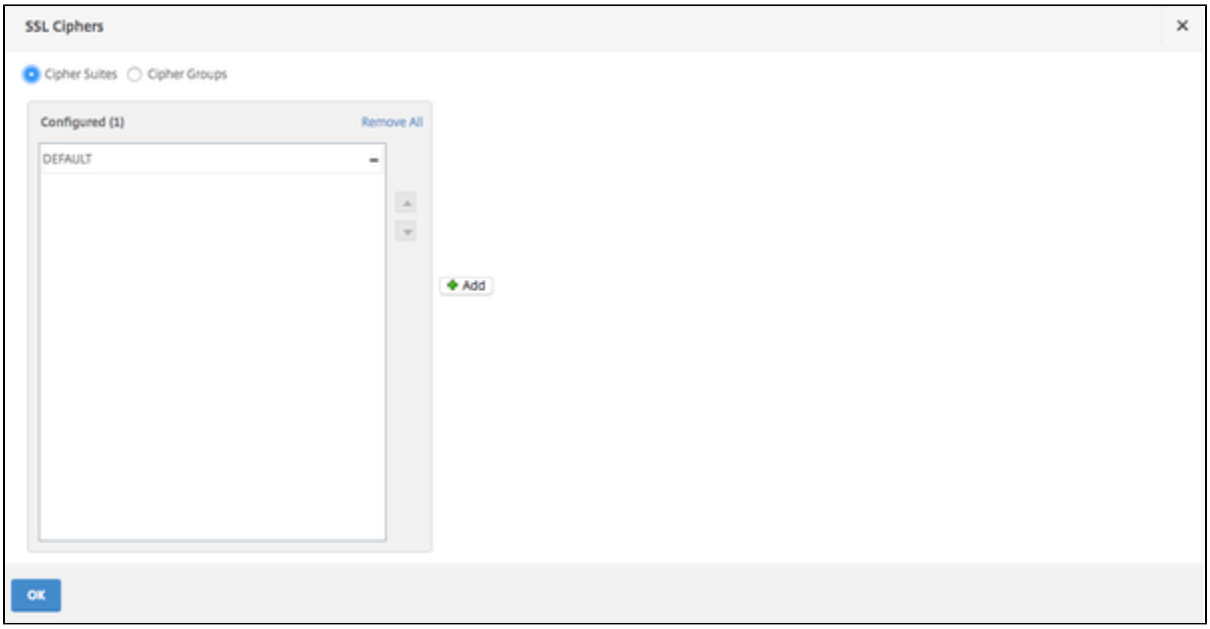
Limit the CipherSuite to be used to PFS (DHE / ECDHE)

If you use default SSL Ciphers or explicitly other than DHE / ECDHE on the Virtual Server setting screen of Traffic Management - Load Balancing - Virtual Servers, disable the corresponding CipherSuite.



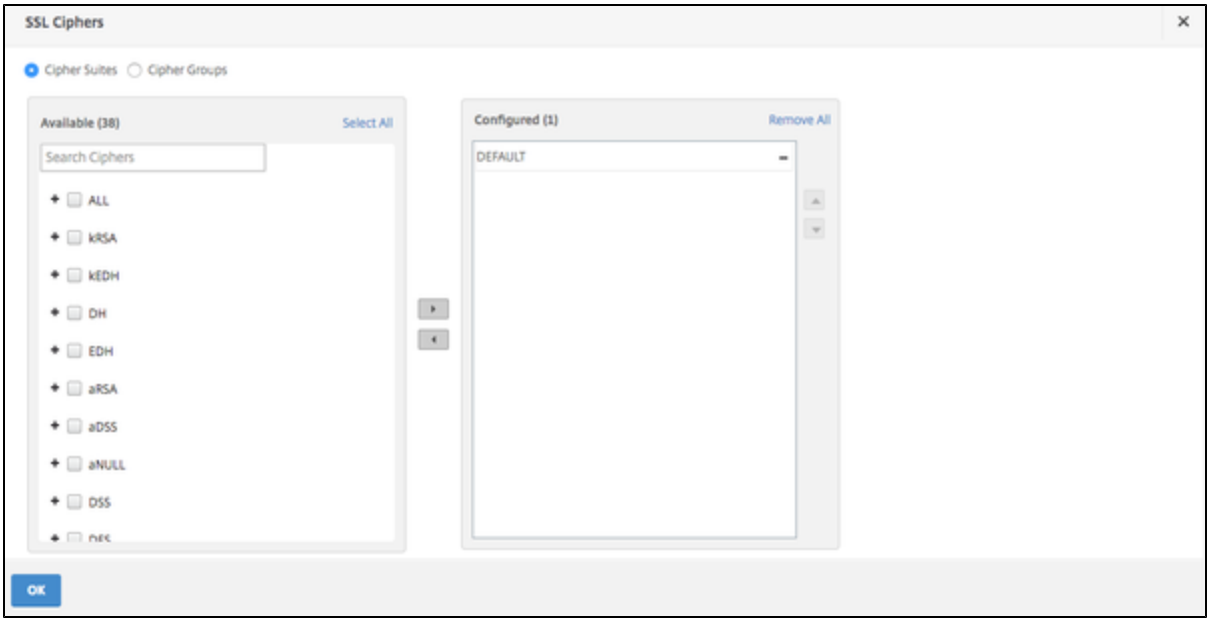


Click the SSL Ciphers edit button and click the Add button in the center.

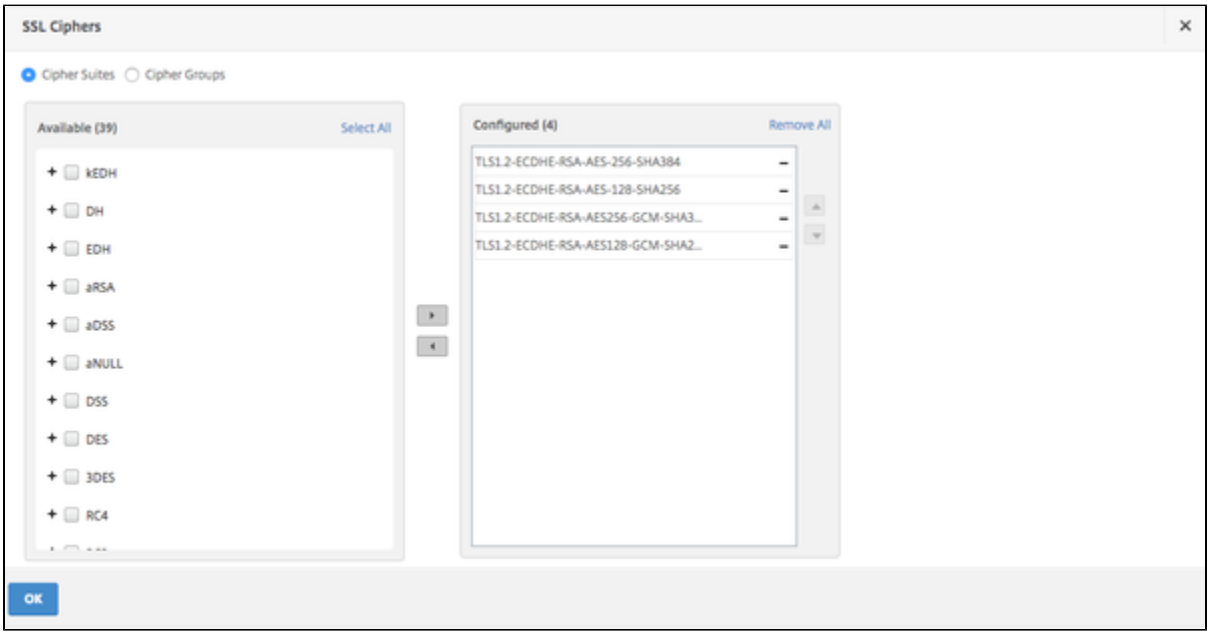


Select the required CipherSuite from Available on the left frame and click on the right direction button at the center to add it.

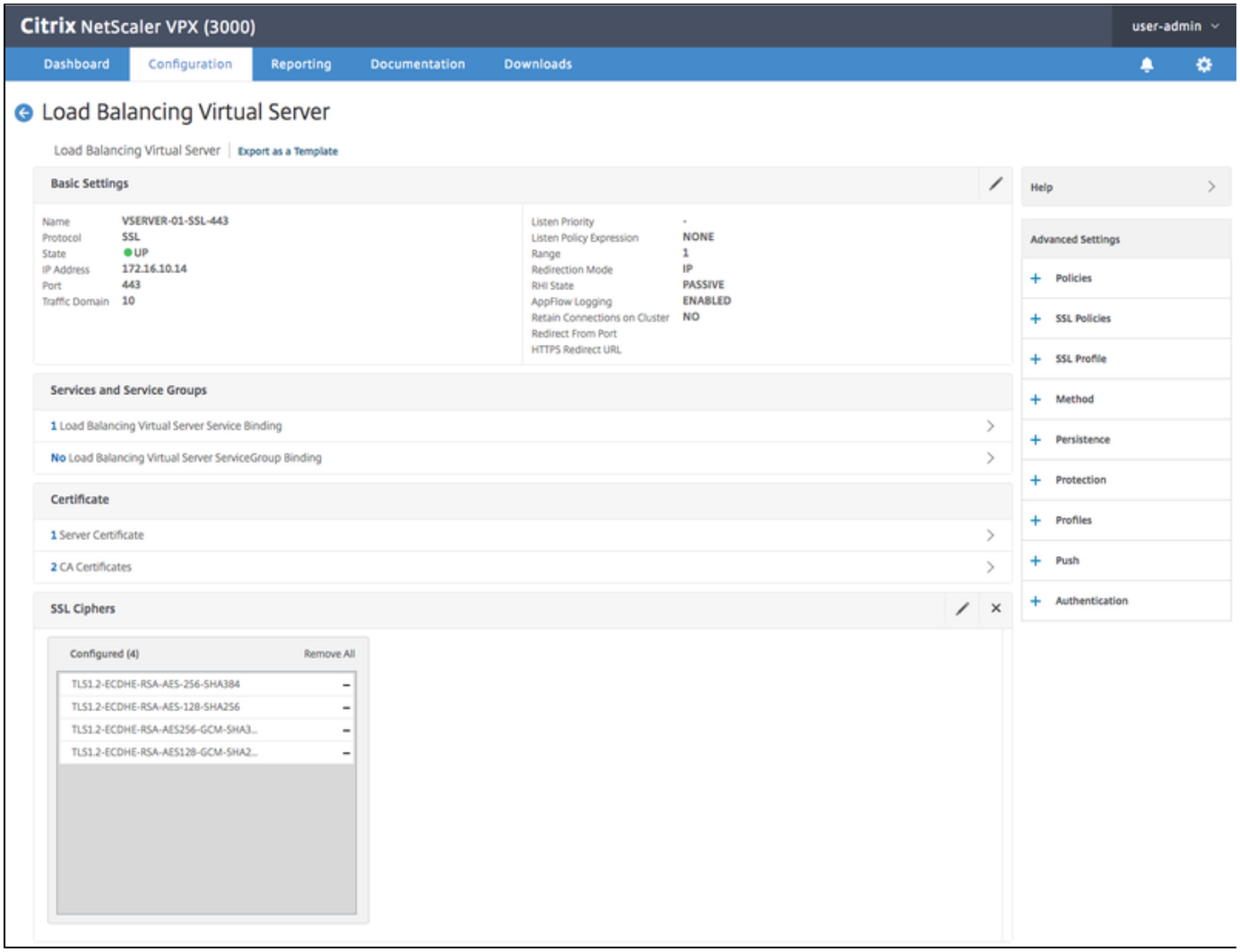
Also, click - on the right side of unnecessary CipherSuite from Configured in the right frame and delete it.



After completing the above, click the OK button (TLS 1.2 - ECDHE - RSA is selected as an example in the screen below).

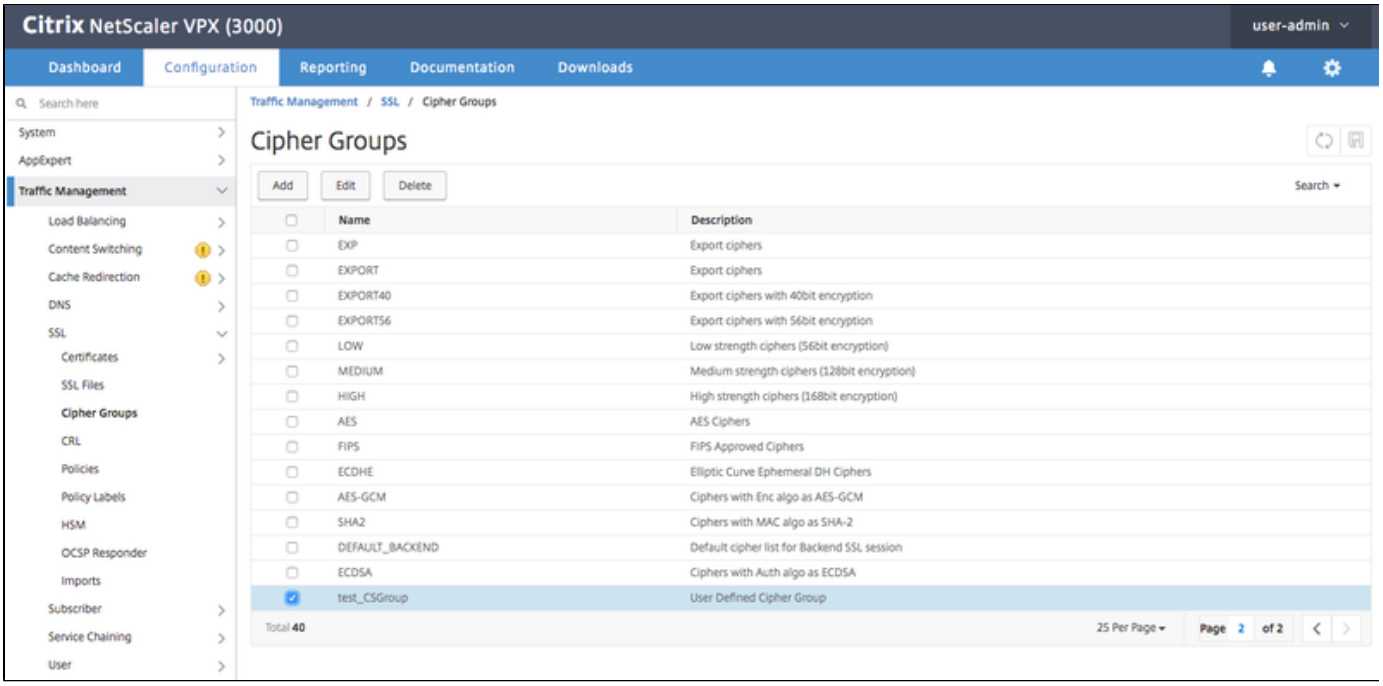


Confirm that settings are reflected correctly and save the settings.

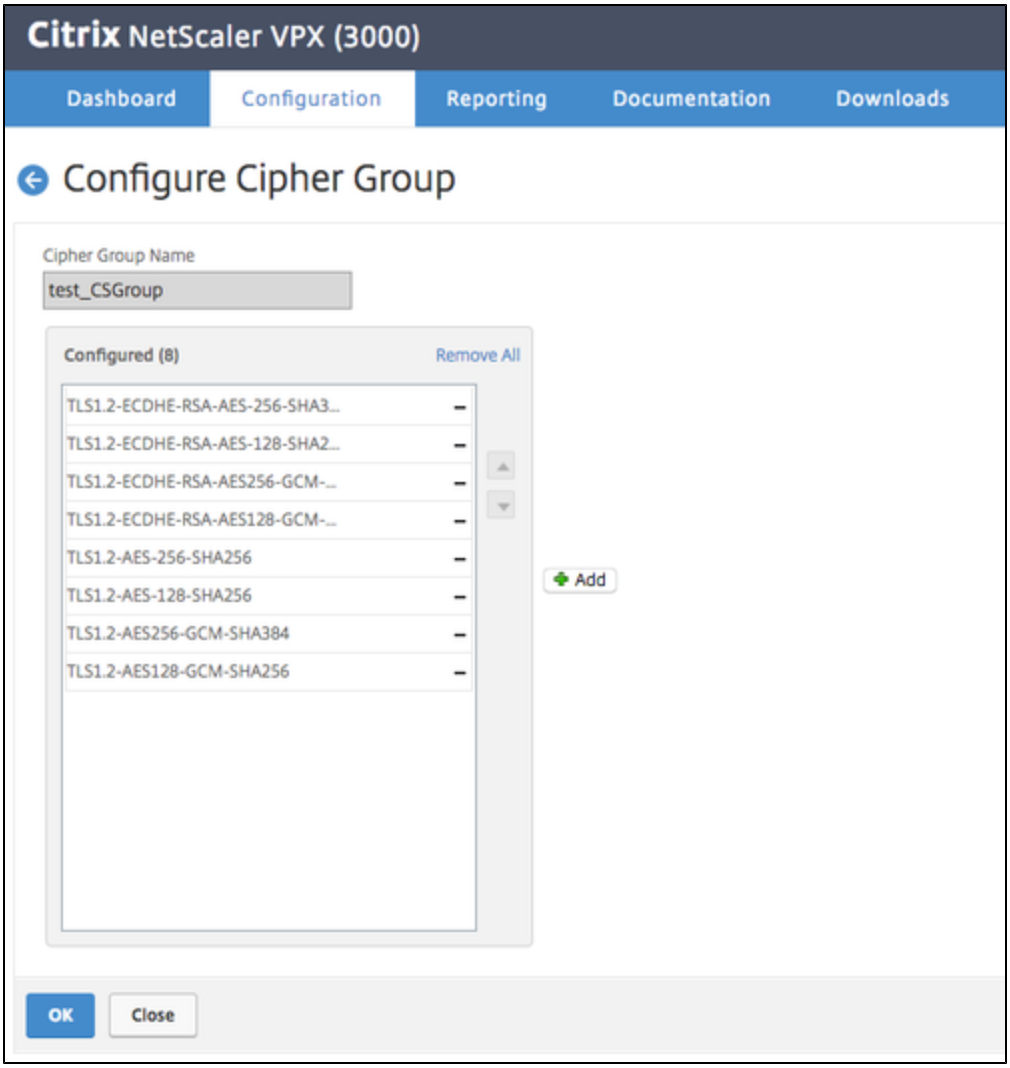


If you create and use CipherGroup including CipherSuite other than DHE / ECDHE, edit the CipherGroup (you can not edit the default Cipher Group, so you need to create a new group).

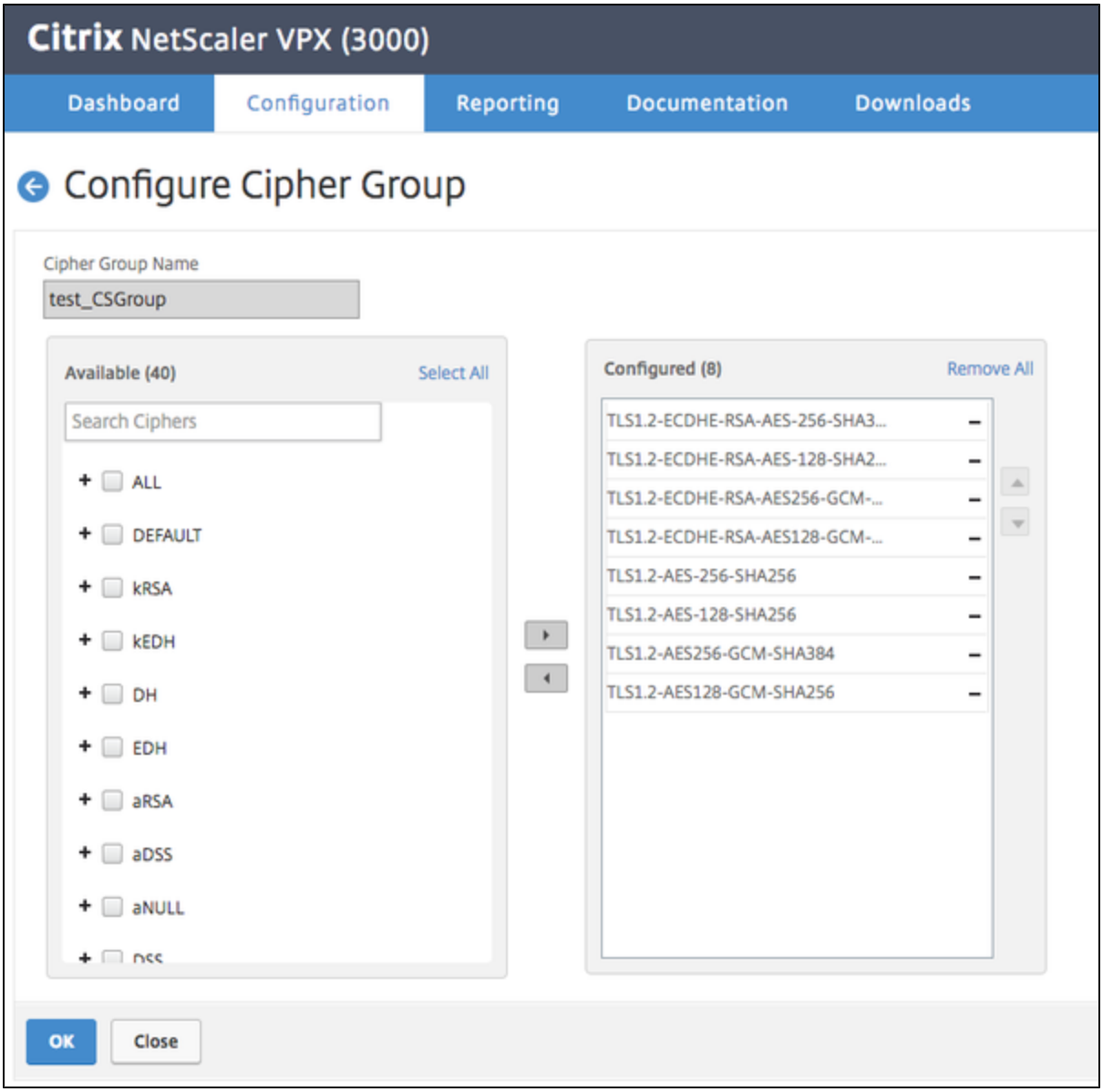
On the Traffic Management - SSL - Cipher Groups screen, select the Cipher Group you are using and click the Edit button.



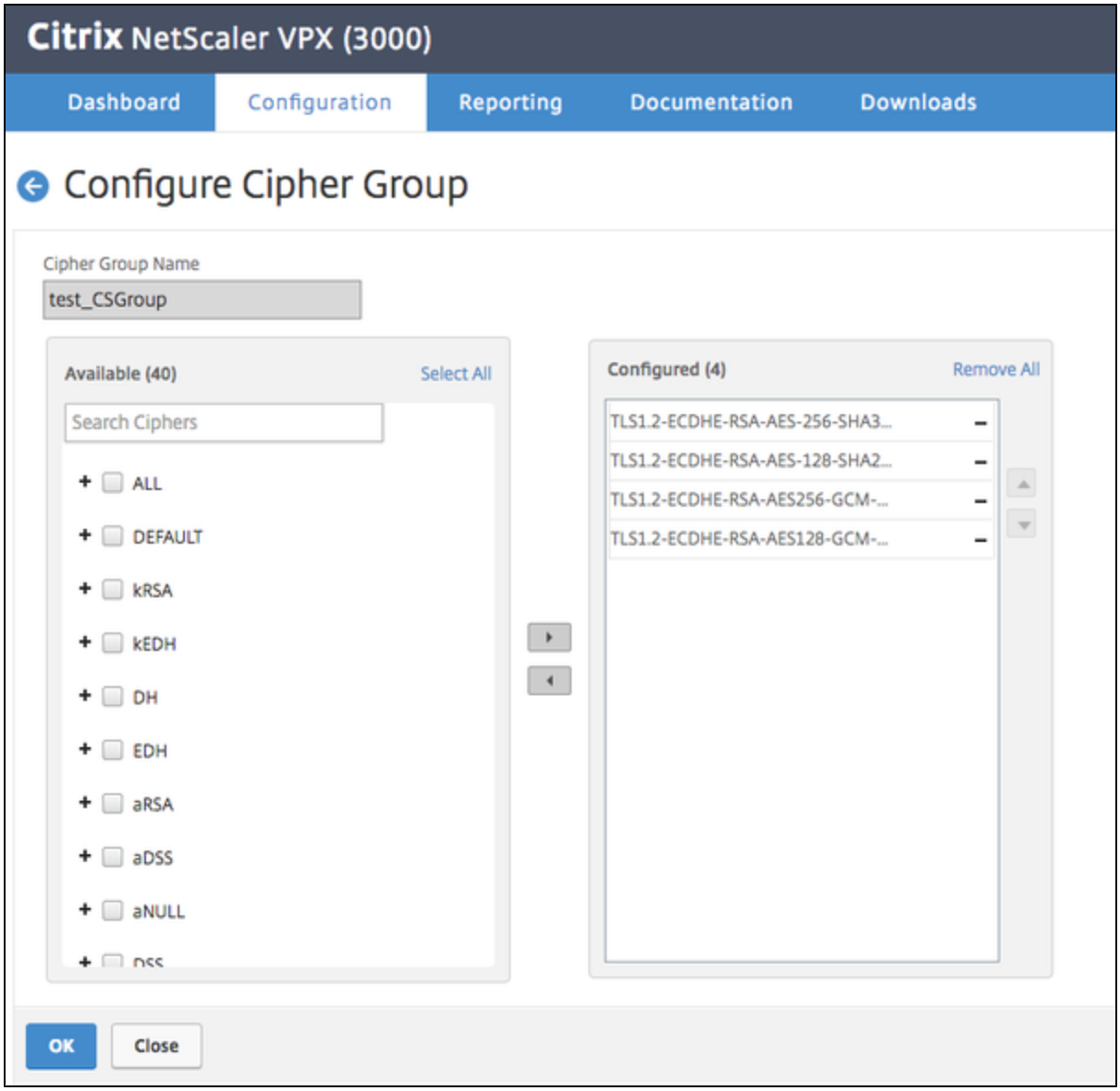
Click the Add button in the center.



From Configured in the right frame, click - on the right side of unnecessary CipherSuite and delete it.



After completing the above, click the OK button (TLS 1.2 - ECDHE - RSA is selected as an example in the screen below).



Setting method via CLI

Limit the CipherSuite to be used to PFS (DHE / ECDHE)

Check the CipherSuite with the SSL setting of VirtualServer.

```
*When using DEFAULT*
bind ssl vserver VSERVER-01-SSL-443 -cipherName DEFAULT

*When specified separately (CipherSuite specified below is an example)*
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES-256-SHA256
Please delete this line.
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES-128-SHA256
Please delete this line.
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES256-GCM-SHA384
Please delete this line.
bind ssl vserver VSERVER-01-SSL-443 -cipherName TLS1.2-AES128-GCM-SHA256
Please delete this line.
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
```

If you use DEFAULT, delete the DEFAULT and set the required CipherSuite by executing the following command.

```
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
```

If specified individually, execute the following command and remove unnecessary CipherSuite.

```
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
```

* When creating and using CipherGroup including other thanDHE/ECDHE.

```
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 5Please delete this line.
bind ssl cipher test_CSGroup -cipherName TLS1.2-AES-128-SHA256
-cipherPriority 6Please delete this line.
bind ssl cipher test_CSGroup -cipherName TLS1.2-AES256-GCM-SHA384
-cipherPriority 7Please delete this line.
bind ssl cipher test_CSGroup -cipherName TLS1.2-AES128-GCM-SHA256
-cipherPriority 8Please delete this line.
```

Execute the following command and remove unnecessary CipherSuite.

```
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
```