

# 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 include PFS (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.

The screenshot shows the Citrix NetScaler VPX (3000) GUI. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The user is logged in as 'user-admin'. The main content area is titled 'Load Balancing Virtual Server' and shows the configuration for a virtual server named 'VSERVER-01-SSL-443'. The 'Basic Settings' section includes fields for Name, Protocol (SSL), State (UP), IP Address (172.16.10.14), Port (443), and Traffic Domain (10). The 'Services and Service Groups' section shows one service binding and no service group bindings. The 'Certificate' section shows one server certificate and two CA certificates. The 'SSL Ciphers' section is highlighted with a red arrow pointing to the 'DEFAULT' cipher suite. The 'Advanced Settings' section on the right includes options for Policies, SSL Policies, SSL Profile, Method, Persistence, Protection, Profiles, Push, and Authentication.

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-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256

**Advanced Settings**

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

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

**SSL Ciphers**

Cipher Suites  Cipher Groups

Configured (1)

Remove All

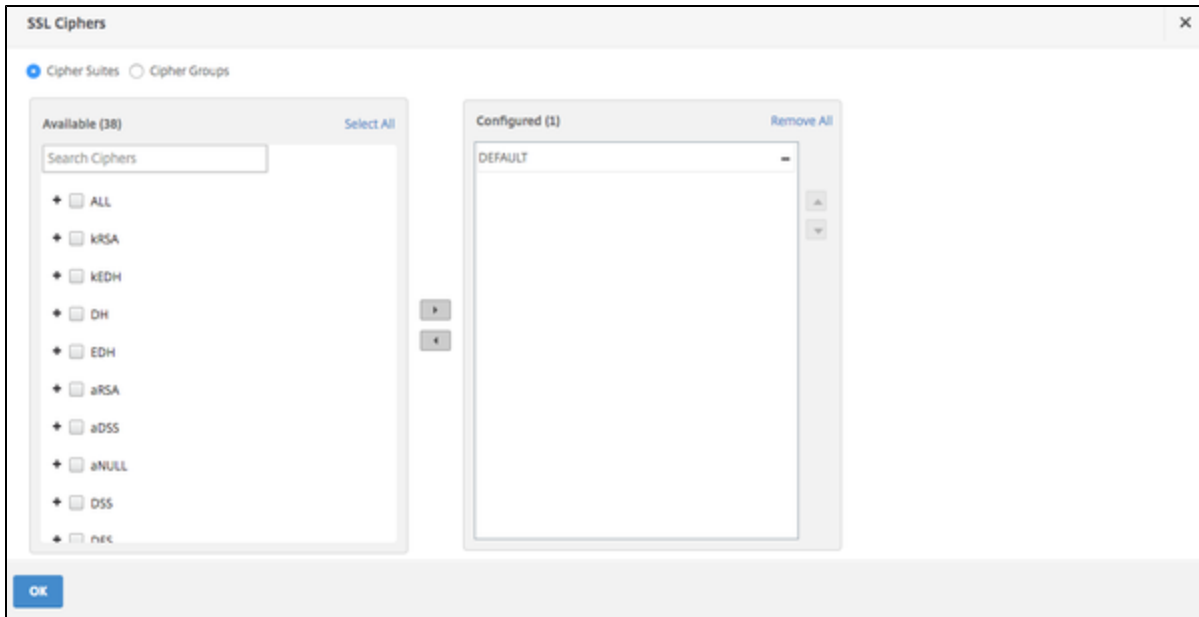
DEFAULT

▲ ▼

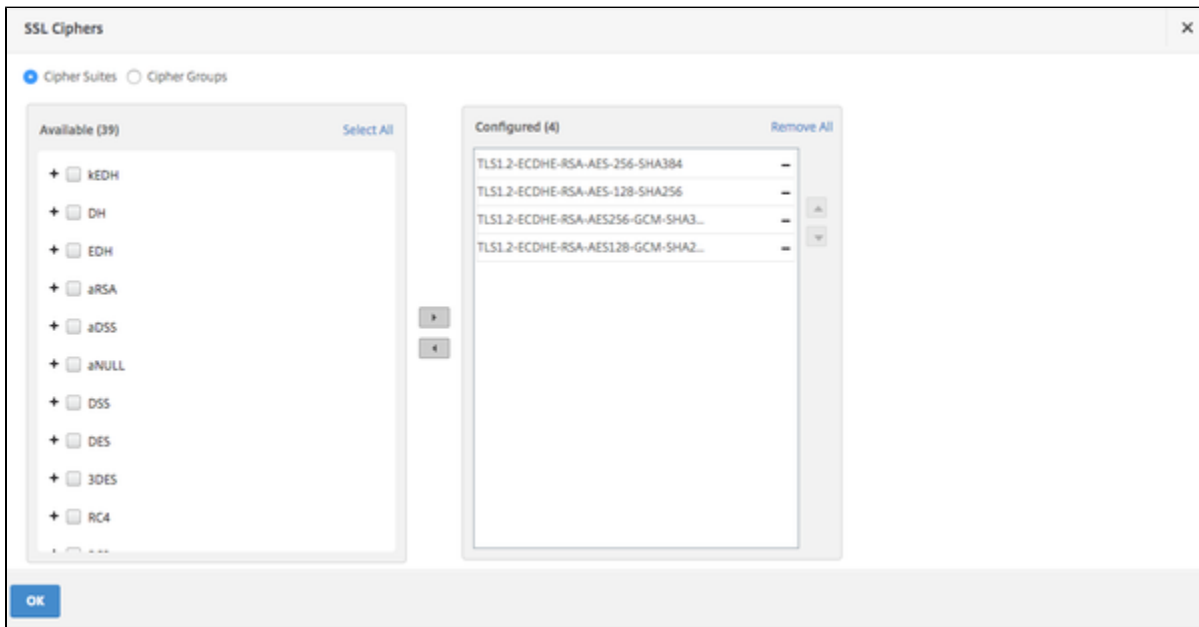
➕ Add

OK

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.

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...

### Help

### Advanced Settings

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

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.

Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

Search here

Traffic Management / SSL / Cipher Groups

### Cipher Groups

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

Click the Add button in the center.

## ← 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

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

**Citrix NetScaler VPX (3000)**

Dashboard Configuration Reporting Documentation Downloads

## ← Configure Cipher Group

Cipher Group Name  
test\_CSGroup

Available (40) [Select All](#)

Search Ciphers

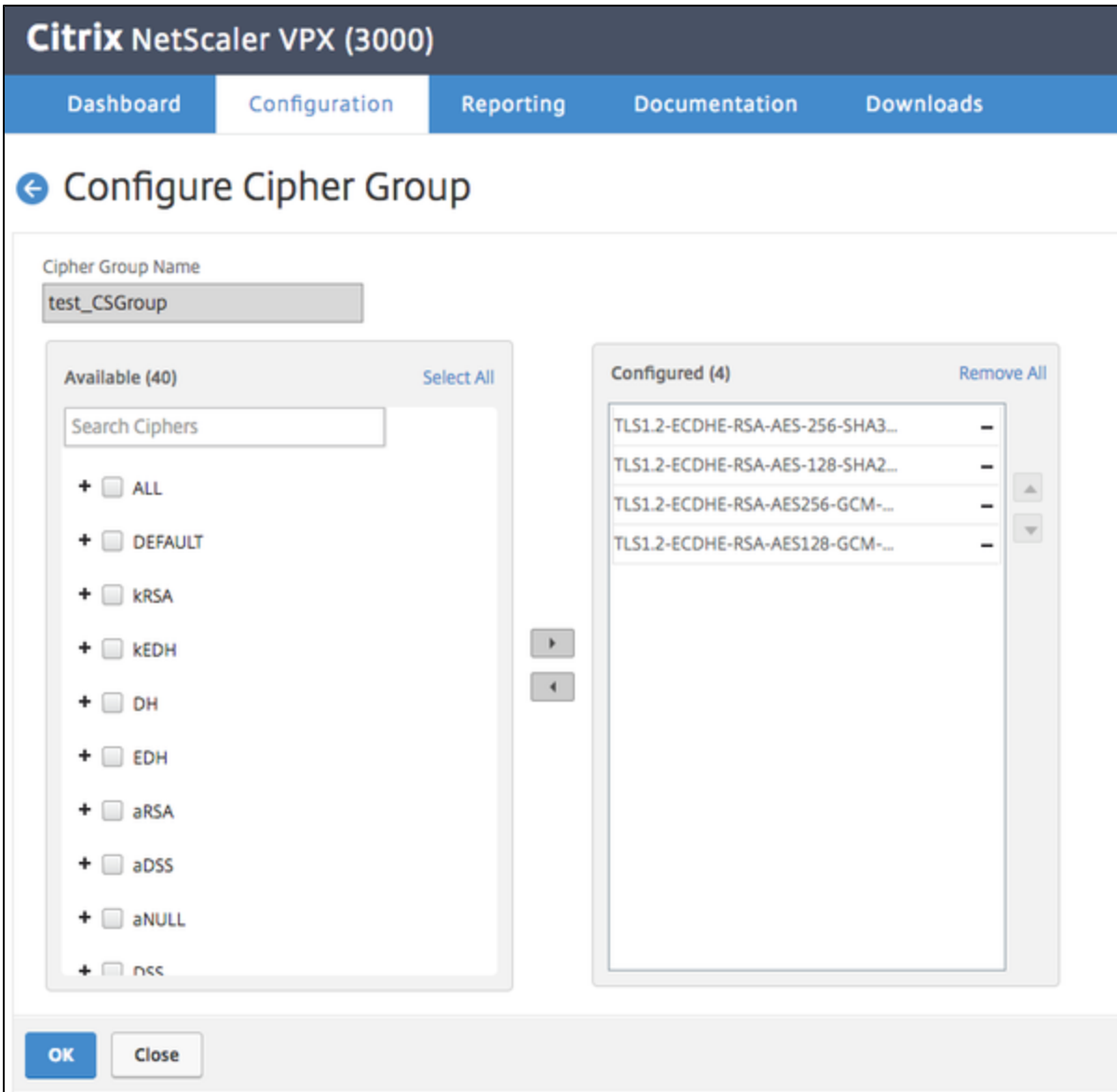
- +  ALL
- +  DEFAULT
- +  kRSA
- +  kEDH
- +  DH
- +  EDH
- +  aRSA
- +  aDSS
- +  aNULL
- +  none

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

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 than DHE/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
```