

# Configure Custom Port for RAVPN on FTD Managed by FMC

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Components Used](#)

### [Configurations](#)

#### [SSL/DTLS Port Change for AnyConnect](#)

#### [IKEv2 Port Change for AnyConnect](#)

### [Verify](#)

### [Troubleshoot](#)

---

## Introduction

This document describes the procedure to configure Custom Port for SSL and IKEv2 AnyConnect on Firepower Threat Defense (FTD) managed by FMC.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Remote Access VPN (RAVPN)
- Experience with Firepower Management Center (FMC)

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco FTD - 7.6
- Cisco FMC - 7.6
- Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configurations

### SSL/DTLS Port Change for AnyConnect

1. Navigate to **Devices > VPN > Remote Access** and **edit** the existing Remote Access policy.

2. Navigate to **Access Interfaces** section and **change** the **Web Access Port Number** and **DTLS Port Number** under **SSL settings** to a port of your choice.

### SSL Settings

Web Access Port Number:*	<input type="text" value="444"/>
DTLS Port Number:*	<input type="text" value="444"/>

*SSL and DTLS Port Change for AnyConnect*

3. **Save** the Configuration.

## IKEv2 Port Change for AnyConnect

1. Navigate to **Devices > VPN > Remote Access** and **edit** the existing Remote Access policy.

2. Navigate to **Advanced** section and then navigate to **IPsec > Crypto Maps**. **Edit** the policy and **change** the Port to your desired port.

The screenshot displays the 'Edit Crypto Map' dialog box in the Cisco AnyConnect configuration interface. The dialog is titled 'Edit Crypto Map' and shows the configuration for the 'FTD-HA-OUTSIDE' interface group. The 'Interface Group' is 'FTD-HA-OUTSIDE'. The 'IKEv2 IPsec Proposals' list contains 'AES-GCM'. The 'Port' field is set to '444'. The 'Enable Reverse Route Injection' and 'Enable Client Services' checkboxes are checked. The 'Enable Perfect Forward Secrecy' checkbox is unchecked. The 'Modulus Group' is '14'. The 'Lifetime Duration\*' is '28800' seconds (Range 120-2147483647). The 'Lifetime Size' is '4608000' Kbytes (Range 10-2147483647). The background shows the 'Advanced' tab of the 'RAVPN\_FTD-HA' configuration page with the 'Crypto Maps' section selected.

*IKEv2 Port Change for AnyConnect*

3. **Save** the Configuration and **Deploy**.



**Note:** When using Custom Port along with AnyConnect Client Profiles, do note that the host address field in the server list must have X.X.X.X:port (192.168.50.5:444) for the connectivity.

---

## Verify

1. Post deployment, the configuration can be verified with the **show run webvpn** and **show run crypto ikev2** commands:

```
<#root>
```

```
>
```

```
show run webvpn
```

```
webvpn
```

```
port 444 <----- Custom Port that has been configured for SSL
```

```
enable outside
```

```
dtls port 444 <----- Custom Port that has been configured for DTLS
```

```
http-headers
  hsts-server
    enable
    max-age 31536000
    include-sub-domains
    no preload
  hsts-client
    enable
  x-content-type-options
  x-xss-protection
  content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-X.X.X.X-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable
```

```
<#root>
```

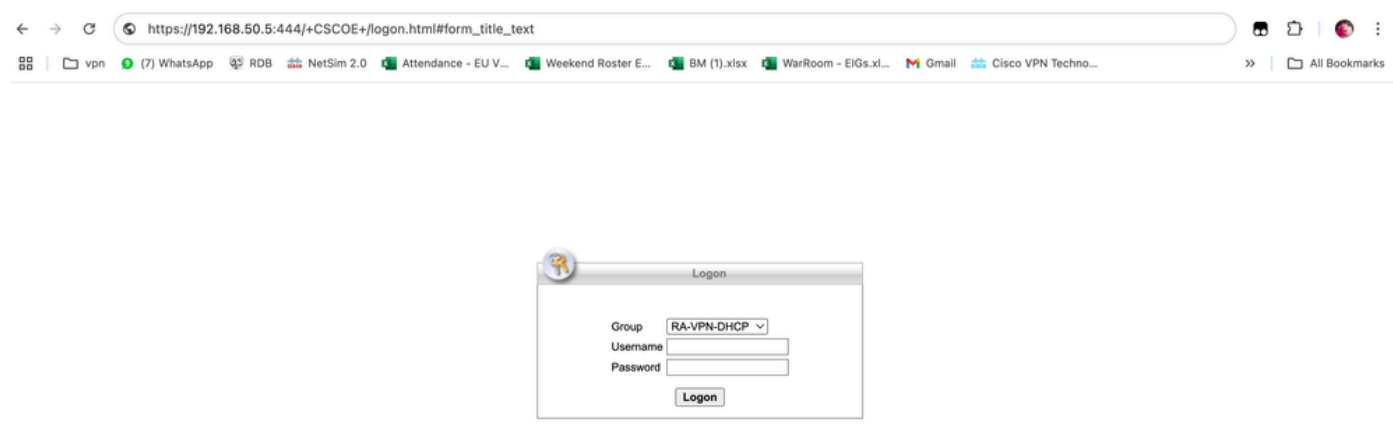
```
>
```

```
show run crypto ikev2
```

```
crypto ikev2 policy 10
  encryption aes-gcm-256 aes-gcm-192 aes-gcm
  integrity null
  group 21 20 19 16 15 14
  prf sha512 sha384 sha256 sha
  lifetime seconds 86400
```

```
crypto ikev2 enable outside client-services port 444 <----- Custom Port configured for IKEv2 Client Serv
```

## 2. Verify by accessing Remote Access from browser/AnyConnect Application with Custom Port:



*Verify by Accessing AnyConnect with Custom Port*

## Troubleshoot

- Ensure that the port used in Remote Access configuration is not used in other services.

- Ensure that the port is not blocked by ISP or any Intermediate devices.
- Captures on FTD can be taken to verify if packets are reaching the firewall and response is being sent or not.