Configure and Troubleshoot WCCP on FTD Using Predefined Template

Contents

Introduction

This document describes the configuration and troubleshooting steps for WCCP on FTD.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Web Cache Communications Protocol (WCCP) version 2 (v2)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Components Used

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

- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat DefenseVirtual(FTDv) v7.4.2

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.
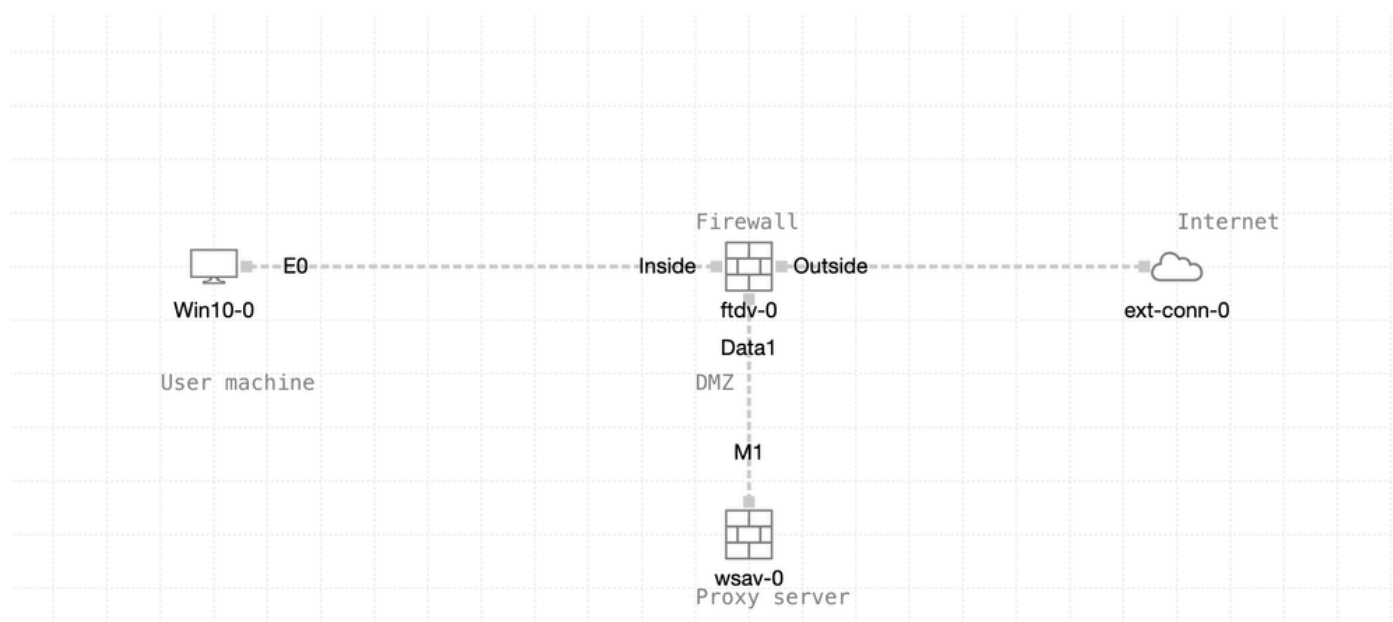
Configure

Web Cache Communication Protocol (WCCP) is used to redirect web traffic to a cache server. It is commonly implemented in network devices such as Cisco routers and firewalls to redirect HTTP, HTTS and FTD over HTTP requests to a proxy server.

WCCP is available in different versions, including WCCP v1, v2, and v3, with each version offering enhanced features and scalability.

How it works

- User machine Win10-0 makes a HTTPS request.
- Here, the FTD Firewall is the gateway for the user PC. It receives the HTTP/HTTPS request.
- FTD understands the destination port is 443 and redirects the traffic to DMZ
- DMZ encapsulates the packet with GRE and forwards the request to Proxy server.
- Proxy server looks into its cache or initiates a new connection to the original server and directly responds to the user machine.
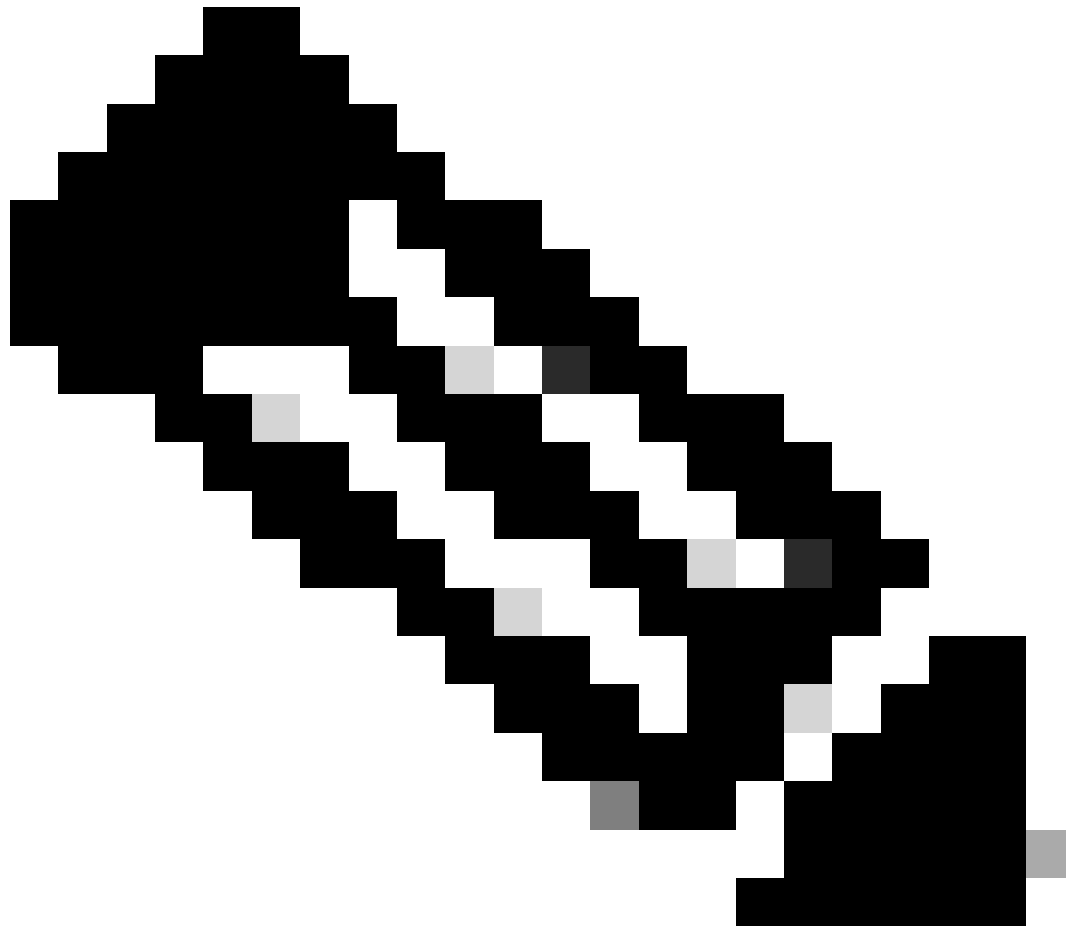
Network Diagram

Network topology

Configurations

These steps demonstrate the configuration for WCCP on FMC. The traffic with port 80 and 443 must be redirected from the **Inside zone** to the **DMZ zone.**

Note: The document describes the steps for dynamic service-id. The port information has been learned from WCCP client.

Step 1: Log in to **FMC GUI** and navigate to **Object > Object Management > Access List > Extended >Add Extended Access List.**

Create two Extended Access Lists.

1) Create Access List to redirect user traffic and click **Save.**

Edit Extended Access List Object
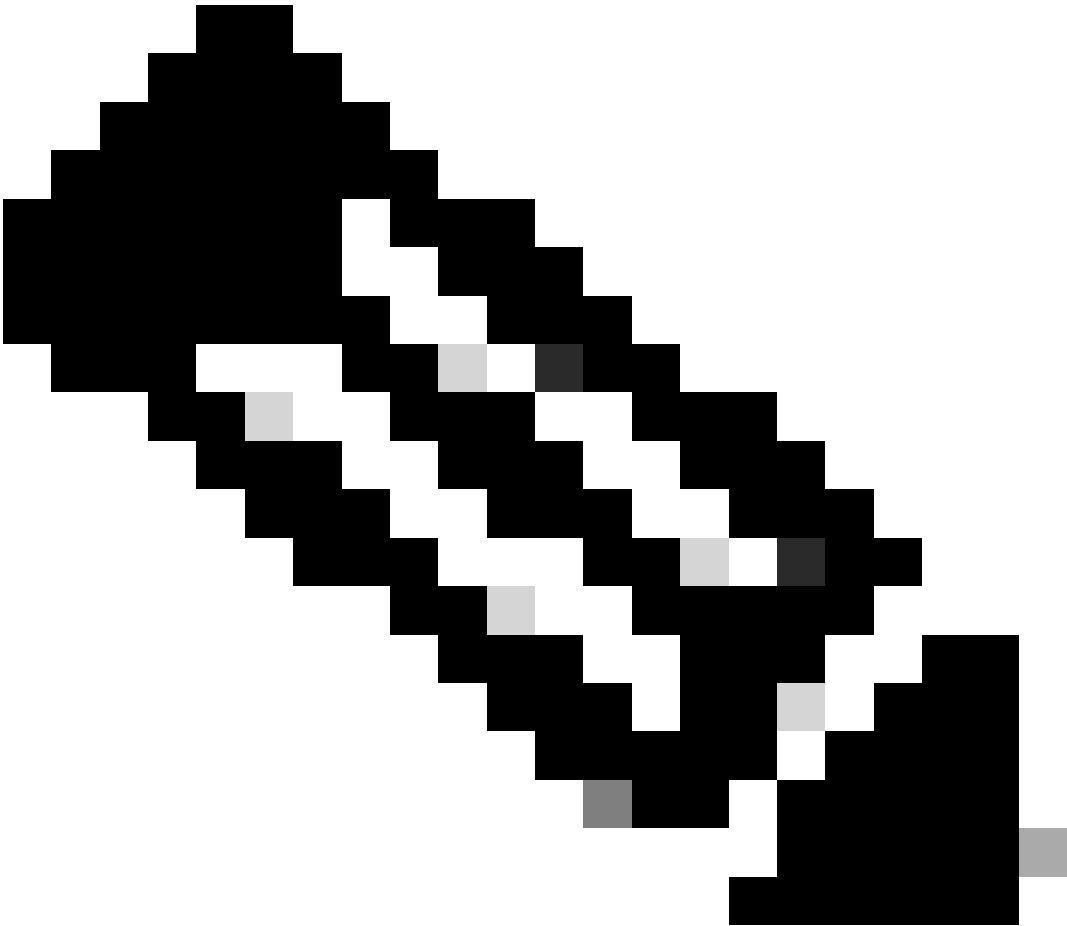
Name
Redirect_traffic

Entries (3)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	🔴 Block	WSA_server	Any	Any	Any	Any	Any	Any	✏️ 🗑️
2	🔴 Block	Any	Any	user_LAN	Any	Any	Any	Any	✏️ 🗑️
3	🟢 Allow	Any	Any	Any	Any	Any	Any	Any	✏️ 🗑️

☐ Allow Overrides

Cancel   Save

Redirect User Traffic

> **Note**: This access-list ensures that you have **Action Block** for traffic coming from WCCP client towards FTD to avoid loop in the network.

Additionally, you can create another statement with **Action Block** to ensure the communication between internal hosts are not sent to proxy server.

The final statement must allow all other traffic that are eligible for redirection to the proxy.

2) Create Access List to identify the WCCP client and click **Save**.

Name

WCCP-CLIENT

Entries (1)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	⊕ Allow	WSA_server	Any	Any	Any	Any	Any	Any	✎ 🗑

☐ Allow Overrides

Cancel   Save

Access List to identify the WCCP client

Note: Configuring an extended access list to include the IP addresses of WCCP server.

Step 2: Navigate to **Object > Object Management > FlexConfig > Text Object > Add Text Object** to add WCCP service and **Save**.

Edit Text Object

Name:

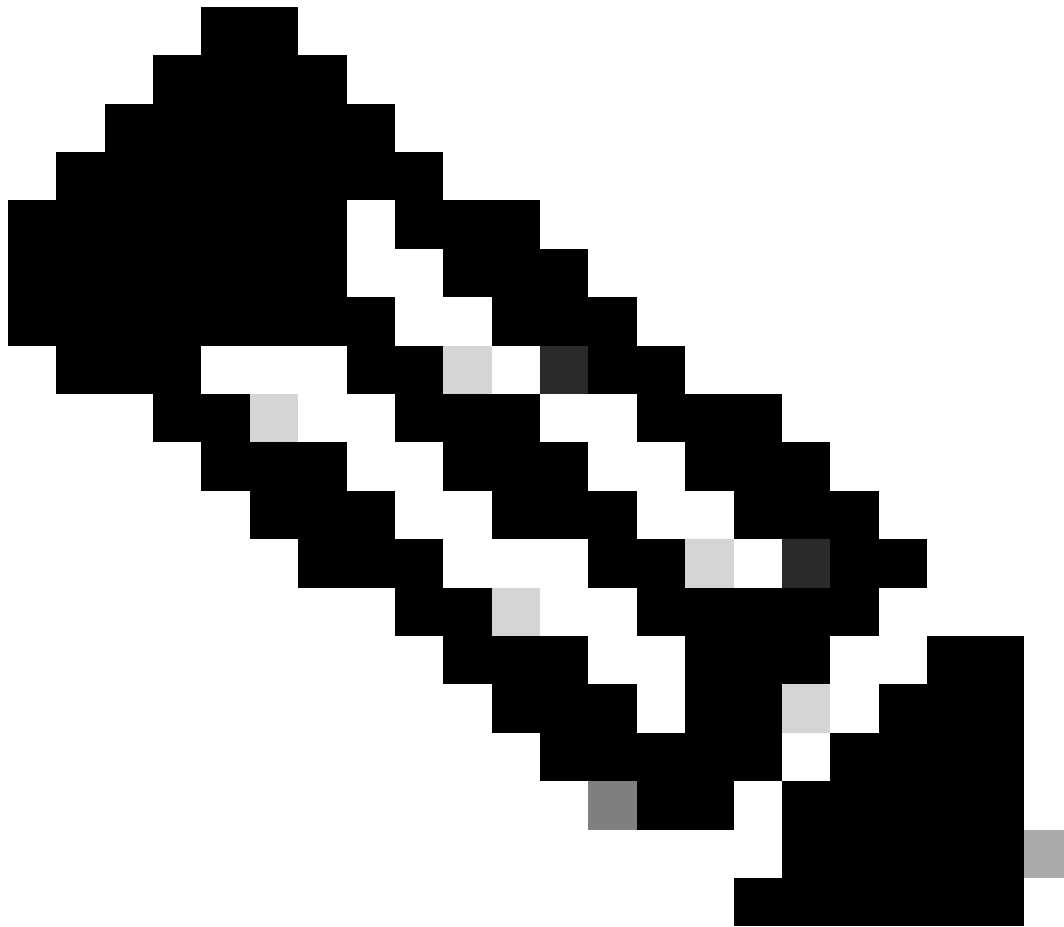wccp-service-object

Description:

Variable Type

Single

Count

1

1	97

☐ Allow Overrides

Cancel   Save

Creating wccp service object

Note: In this example, the service id is 97. It is advisable to select a Service ID between 90 and 97, as these are custom service IDs that typically do not conflict with other service IDs assigned to specific protocols.

For more details, refer to [WCCP on ASA: Concepts, Limitations, and Configuration](#)

Step 3:

- Navigate to **Object > Object Management > FlexConfig > Text Object** and **Search** for **isServiceIdentifer.**

Serach for isServiceIdentifer

- Modify the **isServiceIdentifer** from **false** to **true**.
- **isServiceIdentifer** - When false, uses the standardweb-cacheservice identifier. Refer the

document [Firepower Management Center Configuration Guide](#)

Edit Text Object ?

Name:

isServiceIdentifier

Description:

A flag to identity whether to use
service in wccp.

Variable Type

Single ▼

Count

1 ⬍

1	true

☑ Allow Overrides

▶ Override (0)

Cancel   Save

Modify the value from false to true

Note: Additionally, you can create a user defined **Text Object** shown in Step 2.

Step 4:

- Navigate to **Object > Object Management > Flex Config > FlexConfig Object.**
- **Search** for keyword **wccp**.
- Click the **Clone** option for **Wccp_Configure** template.

Clone the wccp_configure template
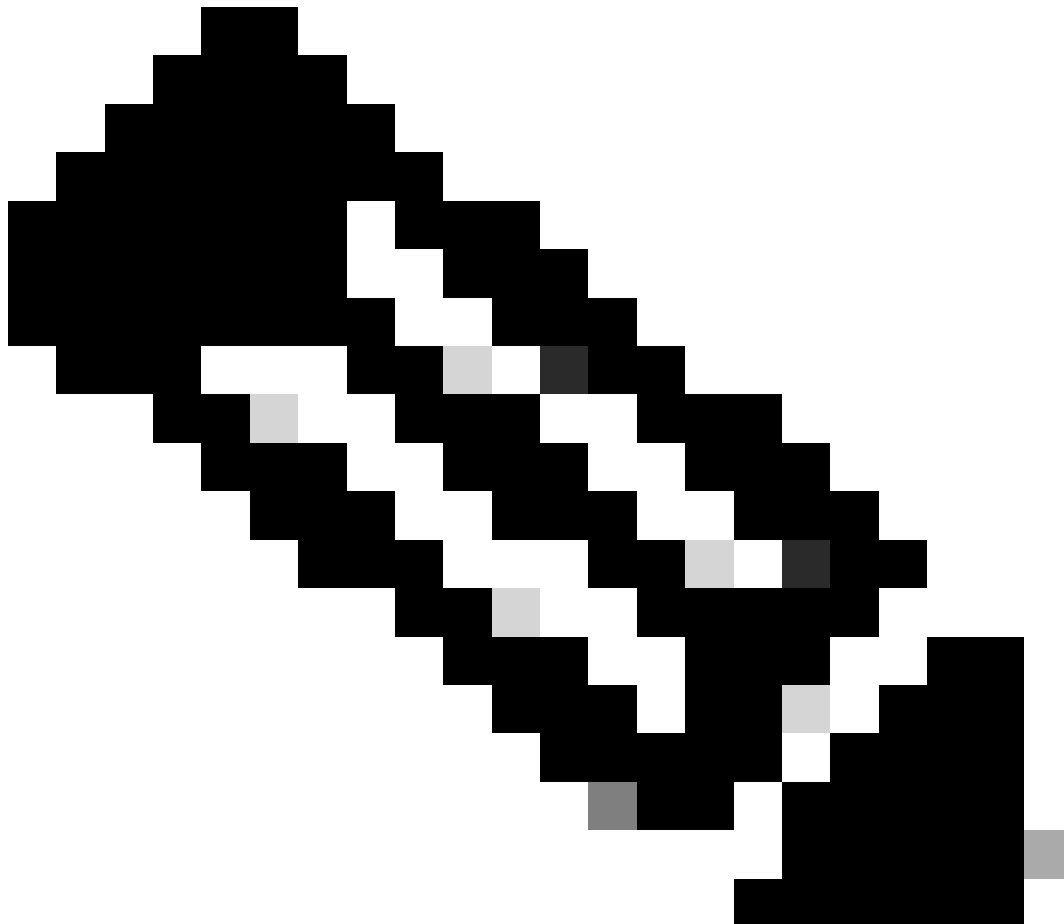
Note: **FlexConfig object** has a predefined template: **Wccp_Configure**. The template cannot be attached to the device. You must **clone** it.

Step 5:

- Remove the **$serviceIdentifier** variables from the third line and provide your own variable.

Remove the service identifier

- Insert the **Text Objectwccp-service** as the variable created in step 2.
- From the drop-down menu, select **Insert > Insert Policy Object > Text Object**

Add FlexConfig Object

Name:

Wccp_Configure_clone

Description:

The template is an example of
wccp configuration. It can not be

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

| Insert ▾ | ⊡ | Deployment: | Once ▾ | Type: | Append |

Insert Policy Object ▶	Text Object
Insert System Variable ▶	Network
Insert Secret Key	Security Zones

```
#set ( $wccpCli = "$wcc          d ACL.
####wccpGroupList is pl          efined in FMC by inserting policy-object of type extended ACL.
####Replace wccpGroupLi    Standard ACL Object
#if( $wccpGroupList )
#set( $wccpCli = "$wccp    Extended ACL Object    >upList")
#end
####wccpRedirectList is    Route Map           r extended ACL.
####Replace wccpRedirectList with extended ACL defined in FMC by inserting policy-object of type extended ACL.
#if( $wccpRedirectList )
#set( $wccpCli = "$wccpCli redirect-list $wccpRedirectList")
#end
```

Inser the wccp-service object as variable

- Provide a **Variable Namewccp-service**.
- Search for **wccp-service-object** in **Available Object**.
- Add the object and **Save** it.

Insert Text Object Variable ❓

Variable Name:

| wccp-service |

Description:

| |

Available Objects ⟳

| 🔍 wccp | ✕ |

| wccp-service-object |
| wccpPassword |

Selected Object

| wccp-service-object | 🗑 |

Add

Cancel **Save**

Add wccp-service object

Step 6:

- Copy the **wccpGroupList** variable name and provide your own variable.

Remove pre-defined wccpGroupList variable

- From drop-down menu **Insert > Insert Policy Object > Extended ACL Object**.

Adding wccpGrouplist Extended ACL

- Paste the name **wccpGroupList** you have copied in previous step in **Variable Name** section.
- Search for **WCCP-CLIENT** in **Available Objects** created in step 1.

- **Add** and **Save** it.

Insert Extended Access List Object Variable

Variable Name:

wccpGroupList

Description:

Available Objects

Search

Redirect_traffic

WCCP-CLIENT

Selected Object

WCCP-CLIENT

Add

Cancel   Save

Add WCCP-CLIENT extended list

Step 7:

- Select **wccpRedirectList** to copy and and provide your own variable.

Add FlexConfig Object

Name:

Wccp_Configure_clone

Description:

The template is an example of
wccp configuration. It can not be

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾ | 🔠 | Deployment: Once ▾ Type: Append

```
#set( $service = "web-cache")
#if( $isServiceIdentifier == "true")
#set( $service = "$wccp-service")
#end
#set ( $wccpCli = "wccp")
#set ( $wccpCli = "$wccpCli $service")
####wccpGroupList is place-holder for extended ACL.
####Replace wccpGroupList with extended ACL defined in FMC by inserting policy-object of type extended ACL.
#if( $wccpGroupList )
#set( $wccpCli = "$wccpCli group-list $wccpGroupList")
#end
####wccpRedirectList is place-holder for extended ACL.
####Replace wccpRedirectList with extended ACL defined in FMC by inserting policy-object of type extended ACL.
#if( $wccpRedirectList )
#set( $wccpCli = "$wccpCli redirect-list $wccpRedirectList")
#end
```

Remove wccpRedirectList

- From the drop-down menu, select **Insert > Insert Policy Object > Extended ACL Object** .

Add FlexConfig Object

Name:

Wccp_Configure_clone

Description:

The template is an example of
wccp configuration. It can not be

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾ | 🔠 | Deployment: Once ▾ Type: Append

Insert Policy Object ▸	Text Object
Insert System Variable ▸	Network
Insert Secret Key	Security Zones

Standard ACL Object

Extended ACL Object

Route Map

```
#set ( $wccpCli = "$wcc
####wccpGroupList is pl          d ACL.
####Replace wccpGroupLi          efined in FMC by inserting policy-object of type extended ACL.
#if(  )
#set( $wccpCli = "$wccp          oupList")
#end
####wccpRedirectList is place-holder for extended ACL.
####Replace wccpRedirectList with extended ACL defined in FMC by inserting policy-object of type extended ACL.
#if( $wccpRedirectList )
#set( $wccpCli = "$wccpCli redirect-list $wccpRedirectList")
#end
```

▼ Variables

Select extedned ACL object for wccpRedirectList

- Paste **wccpRedirectList** in **Variable Name**.
- Search for **Redirect_traffic** in **Available Object**.

- Select **Add** and **Save** it.

Insert Extended Access List Object Variable ?

Variable Name:

wccpRedirectList

Description:

Available Objects ↻

🔍 Search ✕

Redirect_traffic

WCCP-CLIENT

Add

Selected Object

Redirect_traffic 🗑

Cancel   Save

Add Redirect_traffic ACL

Step 8:

- Remove **@wccpPassword**

Removed the pre-defined wccppassword

- Select the Key from the drop down menu **Insert > Insert Secret Key**.

Select secret key

- Click **Add Secret Key**.

Add secret key

- Enter a name in **Secret Key name**.
- Enter the **password**.
- Enter the same password in **Confirm Password** and click **Add**.

Add Secret Key ❓

Secret Key name:*

wccpPassword

Password:*

••••••

Confirm Password *:*

••••••

Cancel   Add

Add user defined secret key

Note: In this example, the inside interface belongs to Security Zone **in**.

Step 9:

- Copy the predefined **security-zone** and replace **$ security-zone** with your own variable.

Edit FlexConfig Object

Name:

Wccp_Configure_clone

Description:

The template is an example of
wccp configuration. It can not

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▼ | 🔳 | Deployment: Once ▼ | Type: Append ▼

```
#set( $wccpCli = "$wccpCli group-list $wccpGroupList")
#end
####wccpRedirectList is place-holder for extended ACL.
####Replace wccpRedirectList with extended ACL defined in FMC by inserting policy-object of type extended ACL.
#if( $wccpRedirectList )
#set( $wccpCli = "$wccpCli redirect-list $wccpRedirectList")
#end

#set( $wccpCli = "$wccpCli password @wccppassword ")

$wccpCli

#### Assiging wccp onto interface
#foreach( $interfaceName in $security-zone)
wccp interface $interfaceName $service redirect in
#end
```

▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
wccpGroupList	SINGLE	WCCP-CLIENT	EXD_ACL:W...	false	
wccp-service	SINGLE	97	FREEFORM:...	false	
interfaceName	SINGLE	in	SECURITYZ...	false	
security-zone	SINGLE	in	SECURITYZ...	false	

Copy the name security-zone

- Select **Security Zones** from the drop-down menu and **Insert > Insert Policy Object**.

Add FlexConfig Object

Name:

Wccp_Configure_clone

Description:

The template is an example of
wccp configuration. It can not be

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

| Insert ▼ | 🔳 | Deployment: | Once | ▼ | Type: | Append |

Insert Policy Object	▶	Text Object	oupList")
Insert System Variable ▶		Network	ded ACL.
Insert Secret Key		Security Zones	L defined in FMC by inserting policy-object of type extended ACL.
#set($wccpCli = "$wccp		Standard ACL Object	RedirectList")
#end		Extended ACL Object	vord ")
#set($wccpCli = "$wccp		Route Map	

$wccpCli

```
#### Assiging wccp onto interface
#foreach( in $security-zone)
wccp interface $interfaceName $service redirect in
#end
```

▼ Variables

Select the security zone

- Paste the **Variable Name** as **security-zone**
- From **Available Objects**, select the interface to **Add**.
- Click **Save**.

Insert Security Zone Variable

Variable Name:

security-zone

Description:

Available Objects

Search

dmz

in

out

Selected Object

in

Add

Cancel   Save

Adding security-zone

Step 10:

- Navigate to **Devices > FlexConfig,** Click **New Policy** or **Edit** an existing policy.
- Select the configured **Wccp_configure_clone** object and click **>** to assign it.
- Click **Save**.

Note: For a New Policy, ensure that you assign the Policy to FTD device. For an existing policy, the policy must have been already assigned.

Assign the configured FlexConfig to device

Step 11: Navigate to **Deploy > Select the FTD Device >** click **Deploy**.

Verify

Step 1: Verify the running configuration.

Log in to FTD CLI and run the command show running-config wccp**.**

Configuration example:

```
wccp 97 redirect-list Redirect_traffic group-list WCCP-CLIENT password *****
wccp interface inside 97 redirect in
```

To ensure the configuration has the correct password, run the commands.

1) system support diagnostic-cli

2) enable

3) Press **Enter** without password

4) more system:running-config | include wccp

Step 2: Verify the WCCP status

Run the command show wccp

```
Global WCCP information:
    Router information:
        Router Identifier:                  -not yet determined-
        Protocol Version:                   2.0

    Service Identifier: 97
        Number of Cache Engines:            1
        Number of routers:                  2
        Total Packets Redirected:           0
        Redirect access-list:               Redirect_traffic
        Total Connections Denied Redirect:  0
        Total Packets Unassigned:           0
        Group access-list:                  WCCP-CLIENT
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
```

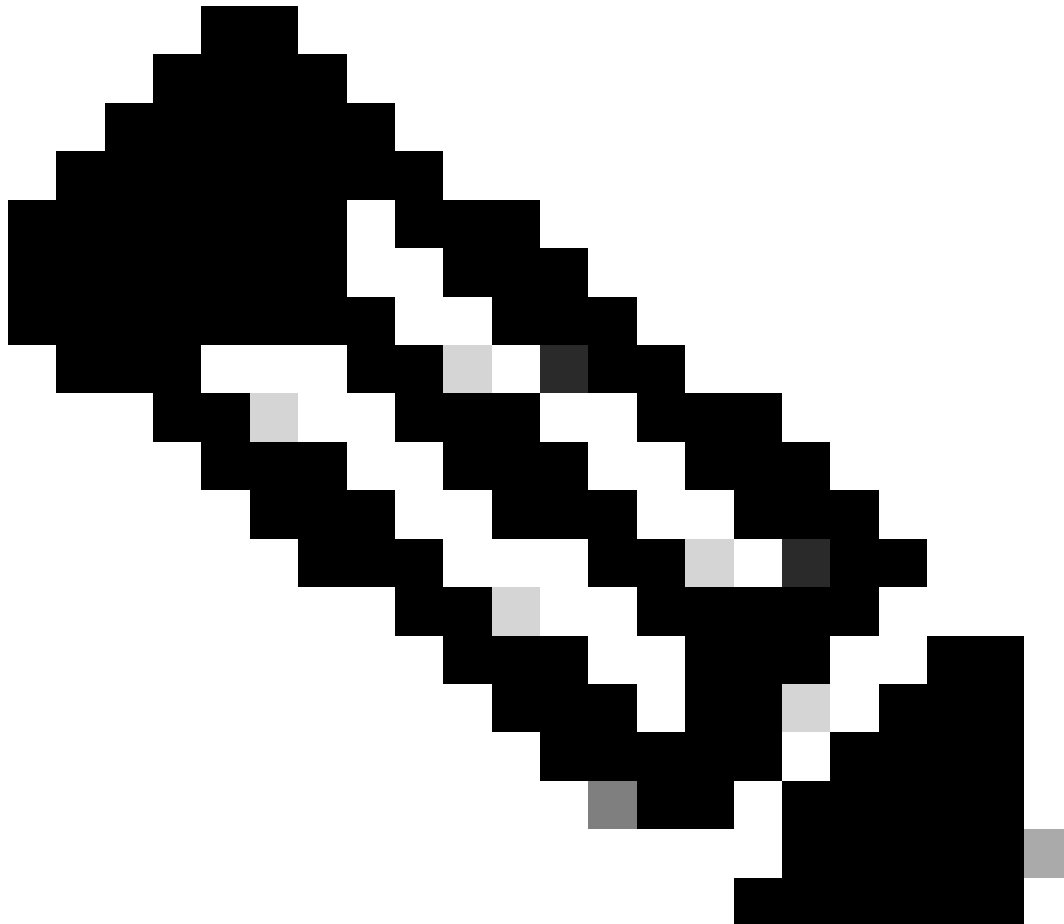 Run the command **show wccp 97 service**

```
WCCP service information definition:
        Type:           Dynamic
        Id:             97
        Priority:       240
        Protocol:       6
```

```
Options:        0x00000012
--------
    Hash:       DstIP
    Alt Hash:   -none-
    Ports:      Destination:: 80 443 0 0 0 0 0 0
```

Note: Here 97 is the service-id. Ensure you can see the port number learned from WCCP client in **Ports:** section.
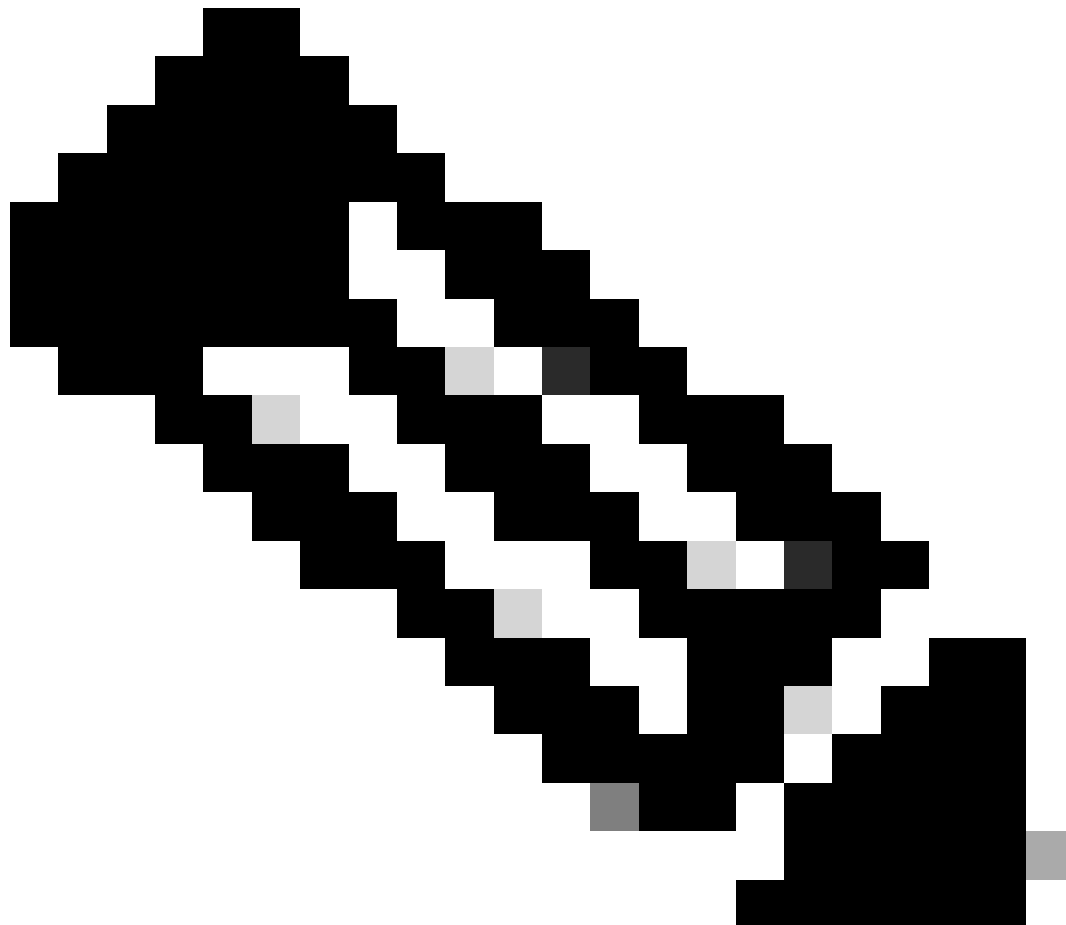
---

3) Run the command show wccp 97 view

Troubleshoot

Step 1: Verify FTD has the route from the same interface that received the WCCP request from Proxy server.

In this example, traffic is redirected to **the**dmz interface.

```
>show route
S        10.xx.xx.xx 255.yyy.yyy.yyy [1/0] via 10.zz.zz.z, dmz
```

Note: Here 10.xx.xx.xx is proxy server IP, 255.yyy.yyy.yyy is Netmask, 10.zz.zz.z is the next hop
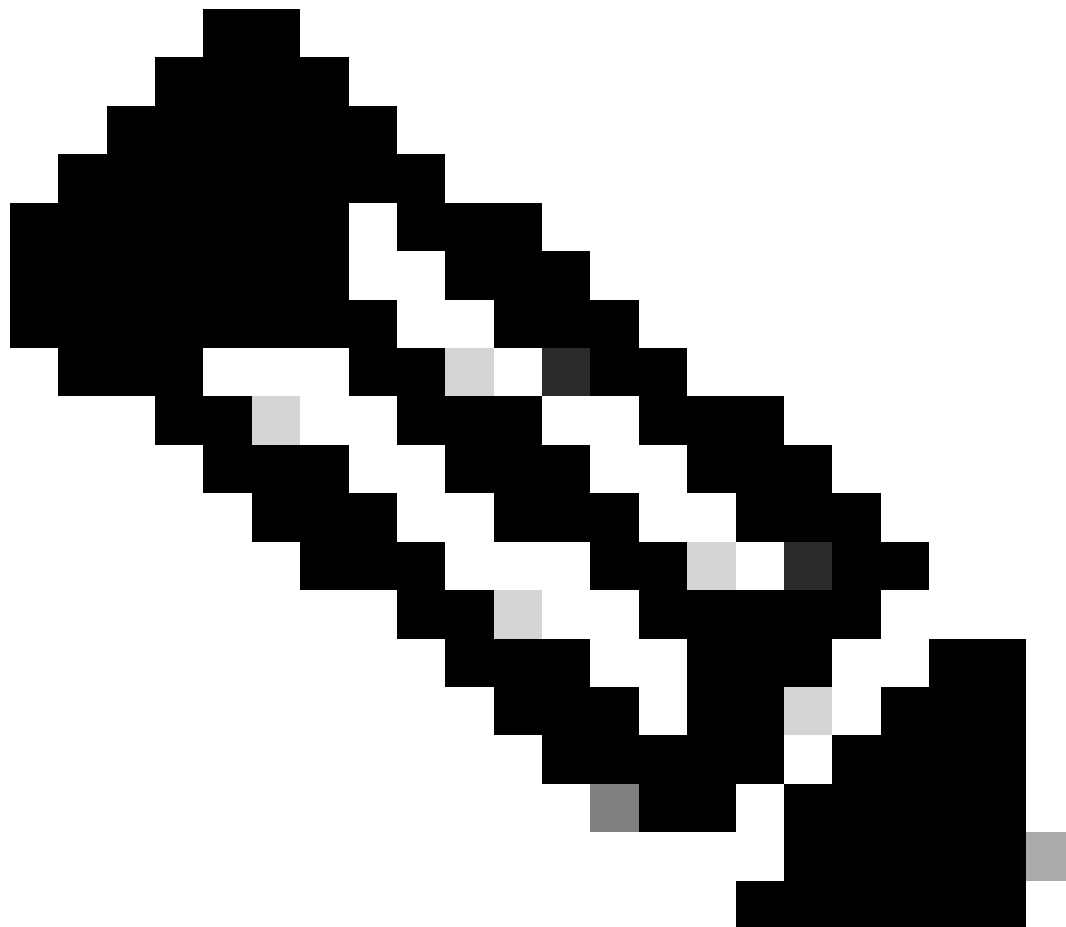gateway.

Step 2: Take the captures on **inside** and **dmz** interface to ensure the traffic is redirected.

Capture on **Inside** interface for port 443

```
capture capinside interface inside trace detail  match tcp any any eq 443
```

Capture on **dmz** interface:

```
capture capdmz interface dmz trace detail match gre any any
```

Note: On **dmz** interface, you must filter with GRE protocol. The redirect packet is encapsulated in GRE packet to wccp client.

Step 3: Debug for wccp

Run the commands:

debug wccp event debu wccp packet

Cisco bug ID<u>CSCvn90518</u> has been raised for enhancement to have the FDM and FMC native mode support for WCCP configuration.