

Configurer et dépanner WCCP sur FTD à l'aide d'un modèle prédéfini

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Comment ça fonctionne](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit les étapes de configuration et de dépannage de WCCP sur FTD.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Centre de gestion du pare-feu sécurisé (FMCv) v7.4.2
- Protection pare-feu sécurisée contre les menaces Virtual(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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

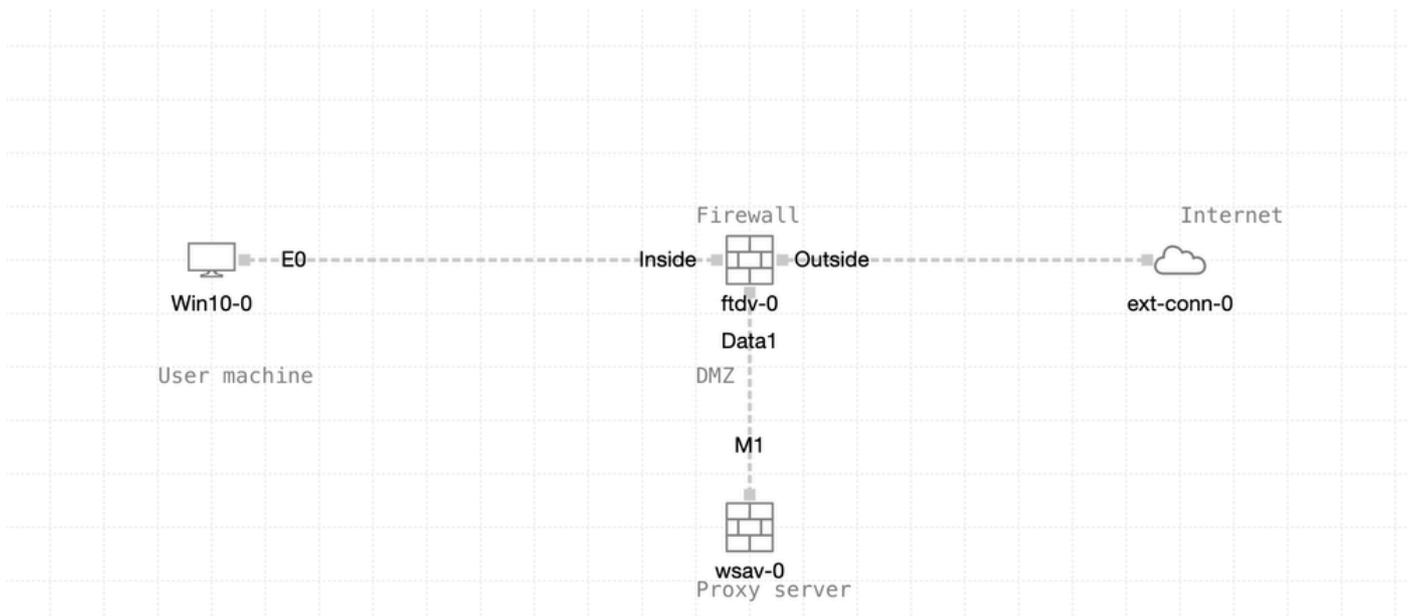
Le protocole WCCP (Web Cache Communication Protocol) est utilisé pour rediriger le trafic Web vers un serveur de cache. Il est généralement mis en oeuvre dans les périphériques réseau tels que les routeurs et les pare-feu Cisco pour rediriger les requêtes HTTP, HTTPS et FTD sur HTTP vers un serveur proxy.

WCCP est disponible dans différentes versions, notamment WCCP v1, v2 et v3, chaque version offrant des fonctionnalités et une évolutivité améliorées.

Comment ça fonctionne

- L'ordinateur utilisateur Win10-0 effectue une requête HTTPS.
- Ici, le pare-feu FTD est la passerelle pour l'ordinateur utilisateur. Il reçoit la requête HTTP/HTTPS.
- FTD comprend que le port de destination est 443 et redirige le trafic vers DMZ
- DMZ encapsule le paquet avec GRE et transfère la requête au serveur proxy.
- Le serveur proxy examine son cache ou initie une nouvelle connexion au serveur d'origine et répond directement à la machine utilisateur.

Diagramme du réseau



Topologie du réseau

Configurations

Ces étapes illustrent la configuration de WCCP sur FMC. Le trafic avec les ports 80 et 443 doit être redirigé de la zone interne vers la zone DMZ.



Remarque : Le document décrit les étapes pour l'ID de service dynamique. Les informations de port ont été apprises à partir du client WCCP.

Étape 1 : Connectez-vous à l'interface utilisateur graphique de FMC et naviguez jusqu'à Object > Object Management > Access List > Extended > Add Extended Access List.

Créez deux listes de contrôle d'accès étendues.

1) Créez une liste d'accès pour rediriger le trafic utilisateur et cliquez sur Enregistrer.

Edit Extended Access List Object



Name

Redirect_traffic

Entries (3)

Add

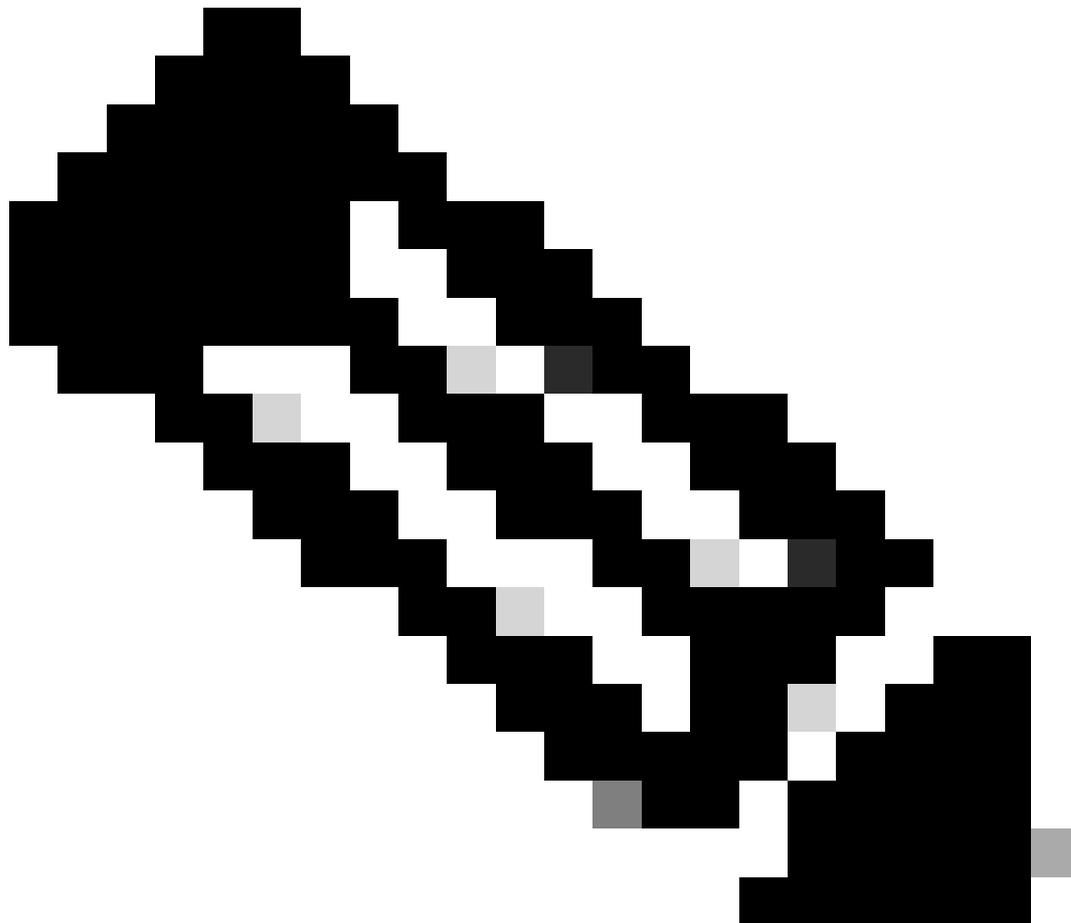
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	WSA_server	Any	Any	Any	Any	Any	Any	
2	Block	Any	Any	user_LAN	Any	Any	Any	Any	
3	Allow	Any	Any	Any	Any	Any	Any	Any	

Allow Overrides

Cancel

Save

Rediriger le trafic utilisateur



Remarque : Cette liste d'accès garantit que vous avez Action Block pour le trafic provenant du client WCCP vers FTD pour éviter la boucle dans le réseau.

En outre, vous pouvez créer une autre instruction avec Action Block pour vous assurer que la communication entre les hôtes internes ne sont pas envoyées au serveur proxy.

L'instruction finale doit autoriser tout autre trafic pouvant être redirigé vers le proxy.

2) Créez une liste d'accès pour identifier le client WCCP et cliquez sur 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

Liste d'accès pour identifier le client WCCP



Remarque : Configuration d'une liste d'accès étendue pour inclure les adresses IP du serveur WCCP.

Étape 2 : Accédez à Object > Object Management > FlexConfig > Text Object > Add Text Object pour ajouter le service WCCP et Enregistrer.

Edit Text Object



Name:

wccp-service-object

Description:

Variable Type

Single

Count

1



1	97

Allow Overrides

Cancel

Save

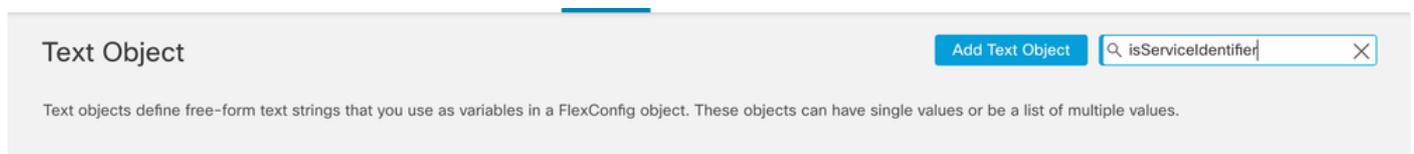


Remarque : Dans cet exemple, l'ID de service est 97. Il est conseillé de sélectionner un ID de service compris entre 90 et 97, car il s'agit d'ID de service personnalisés qui ne sont généralement pas en conflit avec d'autres ID de service attribués à des protocoles spécifiques.

Pour plus de détails, référez-vous à [WCCP sur ASA : Concepts, limites et configuration](#)

Étape 3 :

- Naviguez jusqu'à Object > Object Management > FlexConfig > Text Object et Search for isServiceIdentifier.



Rechercher isServiceIdentifier

- Modifiez isServiceIdentifier de false à true.
- isServiceIdentifier - Si la valeur est false, utilise l'identificateur de service web-cache service standard. Reportez-vous au document [Guide de configuration de Firepower Management Center](#)

Edit Text Object



Name:

isServiceIdentifier

Description:

A flag to identify whether to use service in wccp.

Variable Type

Single

Count

1

1	true

Allow Overrides

► Override (0)

Cancel

Save

Modifiez la valeur de false en true



Remarque : En outre, vous pouvez créer un objet texte défini par l'utilisateur présenté à l'étape 2.

Étape 4 :

- Accédez à Object > Object Management > FlexConfig > FlexConfig Object.
- Recherchez le mot clé wccp.
- Cliquez sur l'option Clone du modèle Wccp_Configure.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ ? admin 🔽 CISCO SECURE

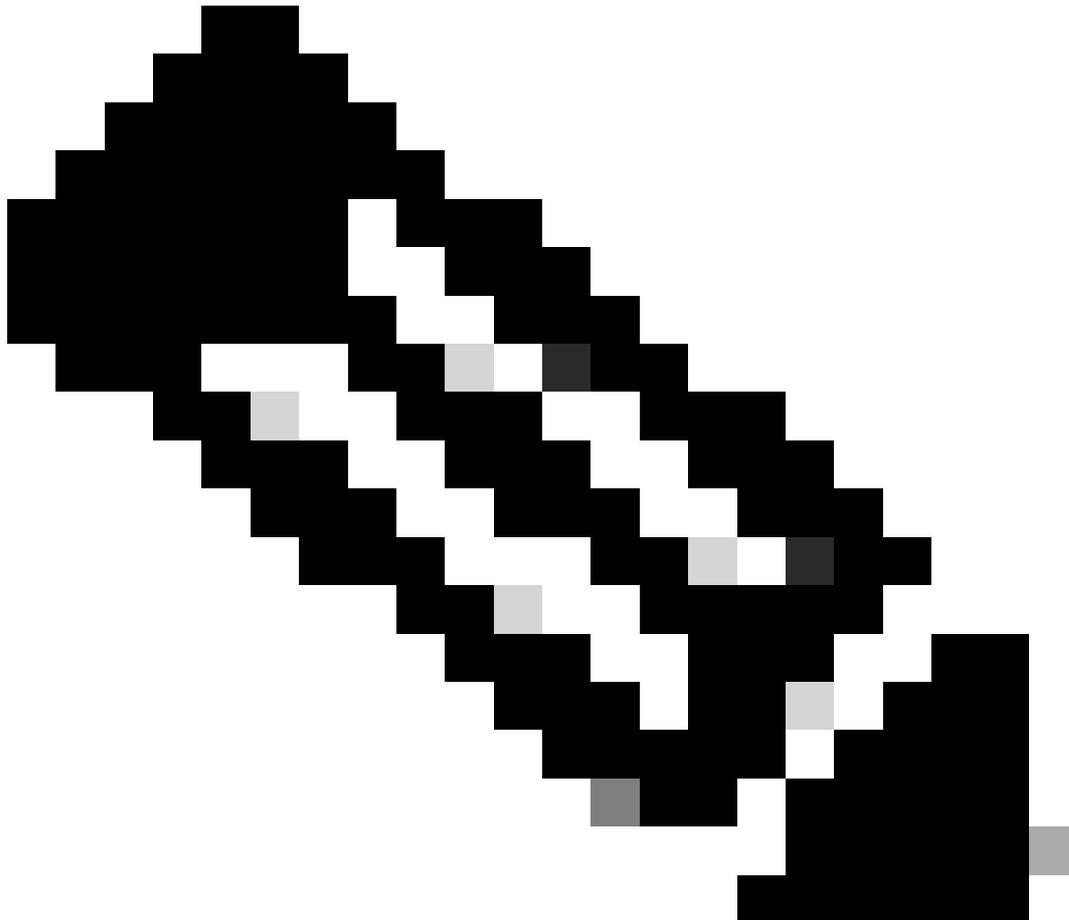
FlexConfig Object

Add FlexConfig Object 🔍 wccp X

FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.

Name	Description	
Wccp_Configure	The template is an example of wccp configur...	 🔍 🗑️
Wccp_Configure_Clear	Clears wccp configurations.	 🔍 🗑️

Clonez le modèle wccp_configure



Remarque : L'objet FlexConfig a un modèle prédéfini : Wccp_Configure. Le modèle ne peut pas être attaché au périphérique. Vous devez le cloner.

Étape 5 :

- Supprimez les variables \$serviceIdentifier de la troisième ligne et fournissez votre propre variable.

Add FlexConfig Object

Name:

Description:

⚠ 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( $service = "$serviceIdentifier")
#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
```

▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
isServiceIdentifier	SINGLE	true	FREEFORM:i...	false	A flag to determine if service ...
serviceIdentifier	SINGLE	1	FREEFORM:...	false	service identifier number is to...

Cancel

Save

Supprimer l'identificateur de service

- Insérez la variable Text Object wccp-service créée à l'étape 2.
- Dans le menu déroulant, sélectionnez 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: | Type:

Insert Policy Object ▸

- Text Object
- Insert System Variable ▸
- Network
- Insert Secret Key
- Security Zones
- Standard ACL Object
- Extended ACL Object
- Route Map

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

Insérez l'objet wccp-service en tant que variable

- Fournissez un service Variable Namewccp-service.
- Recherchez wccp-service-object dans Objet disponible.
- Ajoutez l'objet et enregistrez-le.

Insert Text Object Variable



Variable Name:

Description:

Available Objects 



wccp-service-object

wccpPassword

Add

Selected Object

wccp-service-object



Cancel

Save

Ajouter un objet wccp-service

Étape 6 :

- Copiez le nom de la variable wccpGroupList et fournissez votre propre variable.

Add FlexConfig Object

Name:

Description:

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

Insert Type:

```
#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
```

▼ Variables

Supprimer la variable wccpGroupList prédéfinie

- Dans le menu déroulant Insert > Insert Policy Object > Extended ACL Object.

Add FlexConfig Object

Name:

Description:

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

Insert Type:

Insert Policy Object

- Text Object
- Insert System Variable
- Insert Secret Key
- Network
- Security Zones
- Standard ACL Object
- Extended ACL Object**
- Route Map

```
#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
```

▼ Variables

Ajout de la liste de contrôle d'accès étendue wccpGroupList

- Collez le nom wccpGroupList que vous avez copié à l'étape précédente dans la section Nom

de variable.

- Recherchez WCCP-CLIENT dans Objets disponibles créés à l'étape 1.
- Ajoutez et enregistrez-le.

Insert Extended Access List Object Variable ?

Variable Name:

Description:

Available Objects ↻

✕

- Redirect_traffic
- WCCP-CLIENT**

Selected Object

WCCP-CLIENT 🗑️

Ajouter la liste étendue WCCP-CLIENT

Étape 7 :

- Sélectionnez wccpRedirectList pour copier et fournir votre propre 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
```

Supprimer wccpRedirectList

- Dans le menu déroulant, sélectionnez 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

#set (\$wccpCli = "\$wccpCli \$service")

Standard ACL Object

####wccpGroupList is place-holder for extended ACL.

####Replace wccpGroupList with extended ACL defined in FMC by inserting policy-object of type extended ACL.

#if()

Extended ACL Object

#set(\$wccpCli = "\$wccpCli group-list \$wccpGroupList")

Route Map

#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

Sélectionner un objet ACL étendu pour wccpRedirectList

- Collez wccpRedirectList dans Nom de variable.

- Recherchez Redirect_traffic dans Objet disponible.
- Sélectionnez Ajouter et Enregistrer.

Insert Extended Access List Object Variable ?

Variable Name:

Description:

Available Objects ↻

✕

-  Redirect_traffic
-  WCCP-CLIENT

Selected Object

 Redirect_traffic 🗑️

Ajouter une liste de contrôle d'accès Redirect_traffic

Étape 8 :

- Supprimer **@wccpPassword**

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 ▾

```
####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

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

$wccpCli

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

Suppression du mot de passe wccp prédéfini

- Sélectionnez la clé dans le menu déroulant Insert > Insert Secret Key.

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 ▶

ace-holder for extended ACL.
st with extended ACL defined in FMC by inserting policy-object of type extended ACL.

Insert System Variable ▶

Cli group-list \$wccpGroupList")

Insert Secret Key

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 ")

$wccpCli

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

▾ Variables

Sélectionner la clé secrète

- Cliquez sur Ajouter une clé secrète.

Insert Secret Key ?

[Add Secret Key](#)

	Name	
<input type="checkbox"/>	wccpPassword	 

[Cancel](#) [Save](#)

Ajouter une clé secrète

- Entrez un nom dans Nom de clé secrète.
- Entrez le mot de passe.
- Entrez le même mot de passe dans Confirmer le mot de passe et cliquez sur Ajouter.

Add Secret Key



Secret Key name:*

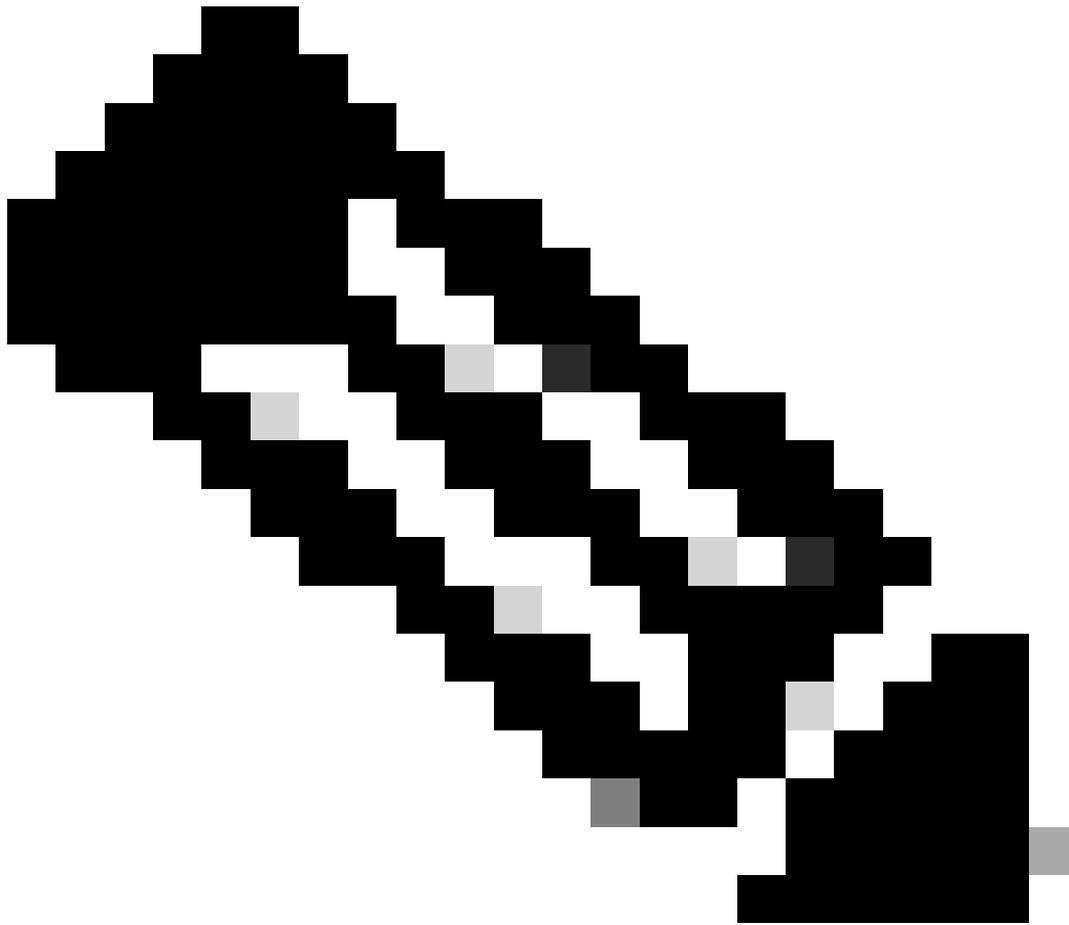
Password:*

Confirm Password *:*

Cancel

Add

Ajouter une clé secrète définie par l'utilisateur



Remarque : Dans cet exemple, l'interface interne appartient à la zone de sécurité dans.

Étape 9 :

- Copiez la zone de sécurité prédéfinie et remplacez `$ security-zone` par votre propre 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  
  
### Assigning 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	

Copiez le nom security-zone

- Sélectionnez Security Zones dans le menu déroulant et 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: ▾ | Type:

Insert Policy Object ▸ | Text Object (groupList")

Insert System Variable ▸ | Network (nded ACL.

Insert Secret Key | Security Zones (defined in FMC by inserting policy-object of type extended ACL.

```
#set( $wccpCli = "$wccp  
#end  
  
#set( $wccpCli = "$wccp  
$wccpCli  
  
#### Assigning wccp onto interface  
#foreach( in $security-zone)  
wccp interface $interfaceName $service redirect in  
#end
```

▼ Variables

Sélectionnez la zone de sécurité

- Collez le nom de variable en tant que zone de sécurité
- Dans Objets disponibles, sélectionnez l'interface à ajouter.
- Cliquez sur Save.

Insert Security Zone Variable



Variable Name:

security-zone

Description:

Available Objects

Search

dmz

in

out

Add

Selected Object

in

Cancel

Save

Ajout d'une zone de sécurité

Étape 10 :

- Accédez à Devices > FlexConfig, cliquez sur New Policy ou Edit an existing policy.
- Sélectionnez l'objet Wccp_configure_clone configuré et cliquez sur > pour l'attribuer.
- Cliquez sur Save.

Remarque : Dans le cas d'une nouvelle stratégie, veuillez à affecter la stratégie au périphérique FTD. Pour une stratégie existante, la stratégie doit avoir déjà été attribuée.

WCCP_config
Enter Description

Migrate Config Preview Config Save Cancel

Policy Assignments (1)

Available FlexConfig FlexConfig Object

User Defined

- Wccp_Configure_clone

System Defined

- Default_DNS_Configure
- Default_Inspection_Protocol_Disable
- Default_Inspection_Protocol_Enable
- DHCPv6_Prefix_Delegation_Configure
- DHCPv6_Prefix_Delegation_UnConfigure
- DNS_Configure
- DNS_UnConfigure
- Eigrp_Configure
- Eigrp_Interface_Configure
- Eigrp_UnConfigure
- Eigrp_Unconfigure_All

Selected Prepend FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	Wccp_Configure_clone	The template is an example of wccp configuration. It can not be used as it is for deployment. User needs to copy this, modify text-object and create objects expected by the templa...

Attribuez la configuration FlexConfig configurée au périphérique

Étape 11 : Accédez à Déployer > Sélectionnez le périphérique FTD > cliquez sur Déployer.

Vérifier

Étape 1 : Vérifiez la configuration en cours.

Connectez-vous à l'interface de ligne de commande FTD et exécutez la commande `show running-config wccp`.

Exemple de configuration :

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

Pour vous assurer que la configuration dispose du mot de passe correct, exécutez les commandes.

- 1) `system support diagnostic-cli`
- 2) `enable`
- 3) Appuyez sur Entrée sans mot de passe
- 4) `more system:running-config | include wccp`

Étape 2 : Vérification de l'état WCCP

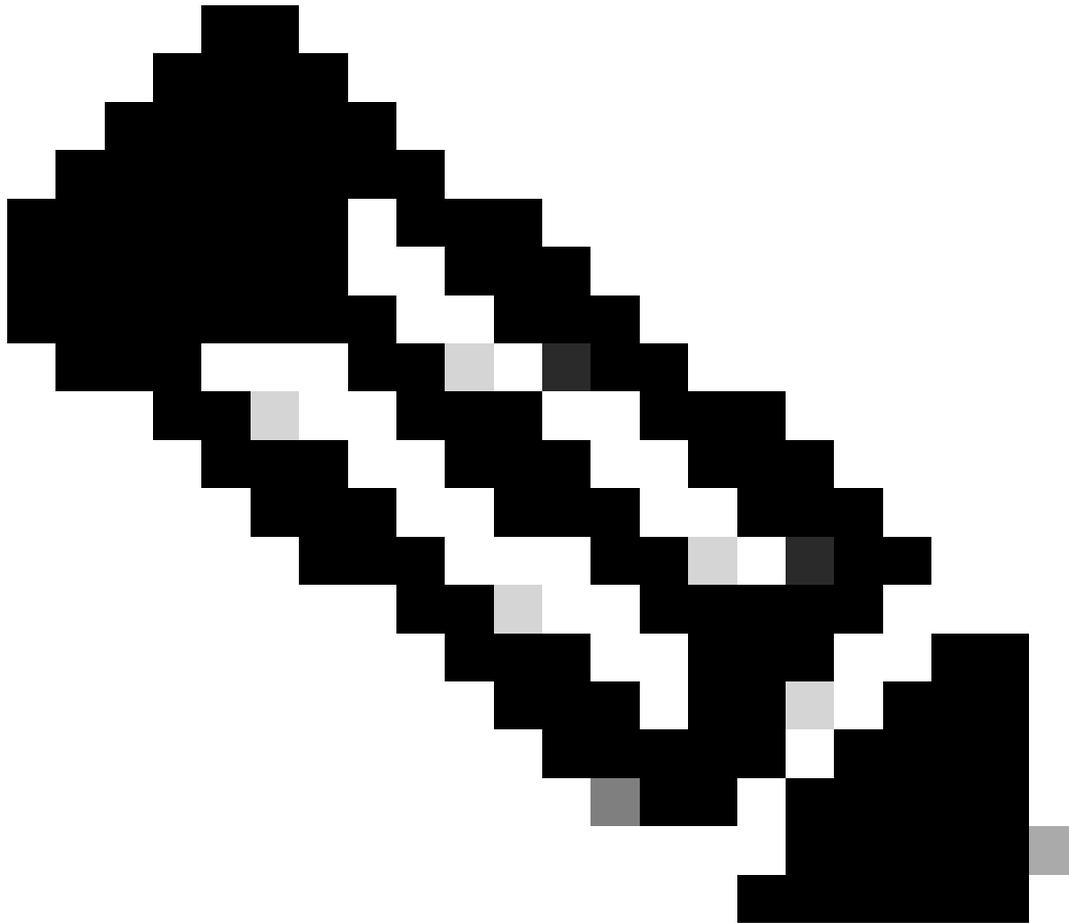
Exécutez la commande `show wccp`

```
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
```

Exécutez la commande `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
```



Remarque : Ici, 97 est l'ID de service. Assurez-vous que vous pouvez voir le numéro de port appris du client WCCP dans Ports : de l'Aide.

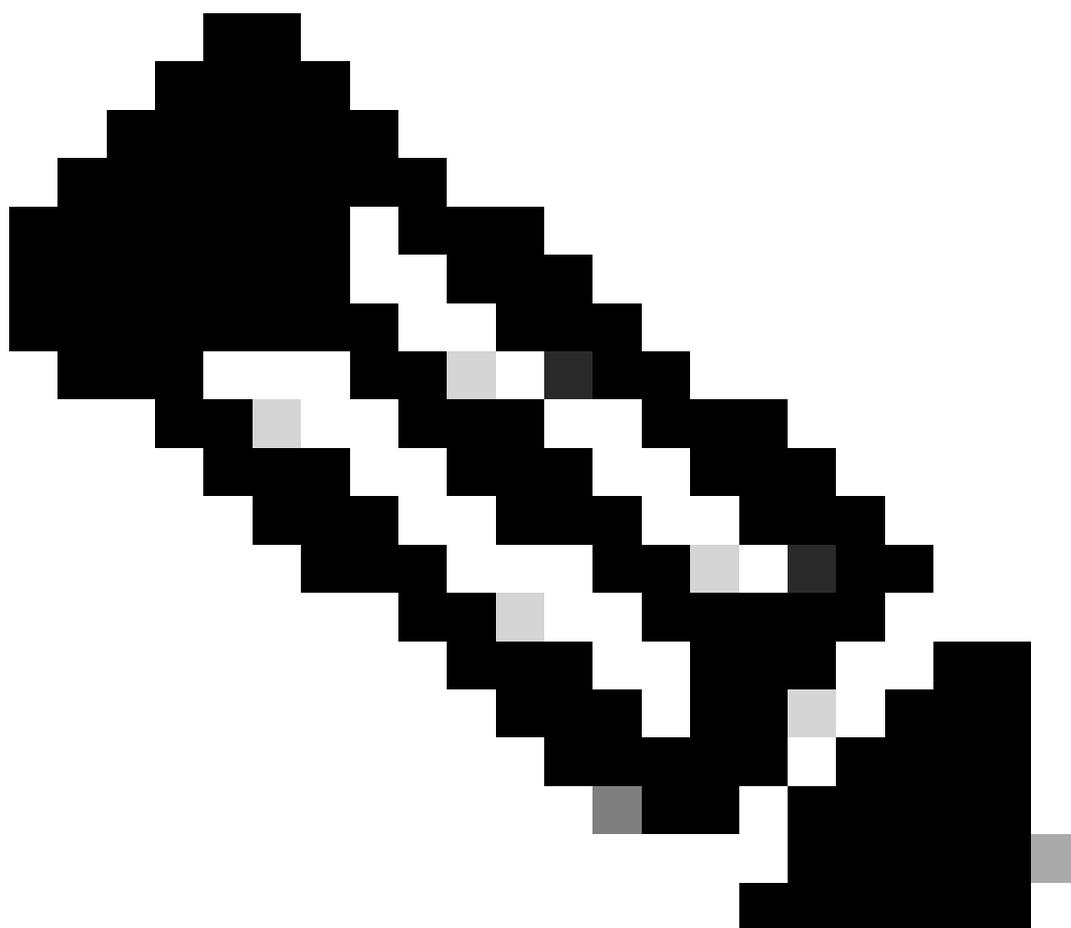
3) Run the command `show wccp 97 view`

Dépannage

Étape 1 : Vérifiez que FTD dispose de la route provenant de la même interface que celle qui a reçu la requête WCCP du serveur proxy.

Dans cet exemple, le trafic est redirigé vers l'interface dmz.

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



Remarque : Ici 10.xx.xx.xx est l'adresse IP du serveur proxy, 255.yyy.yyy.yyy est le masque de réseau, 10.zz.zz.z est la passerelle de tronçon suivant.

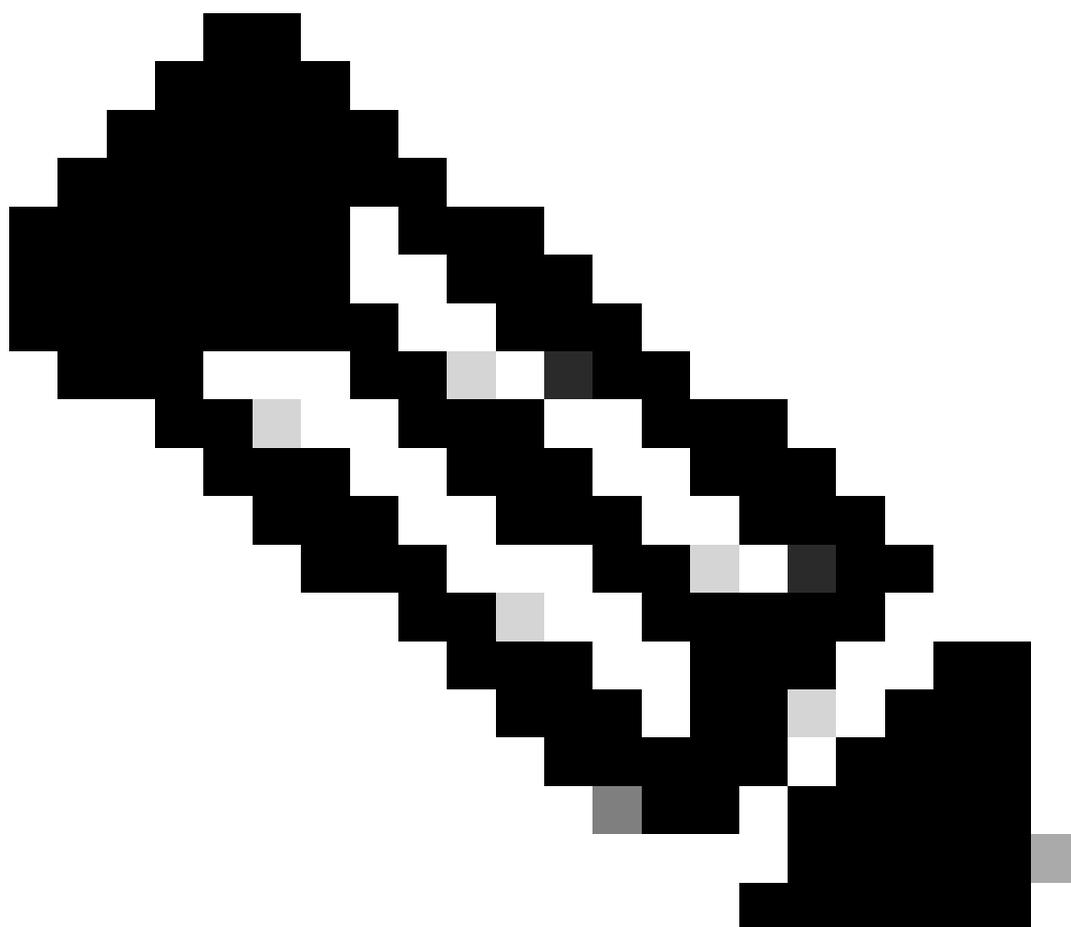
Étape 2 : Prenez les captures sur l'interface interne et dmz pour vous assurer que le trafic est redirigé.

Capture sur l'interface interne pour le port 443

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

Capture sur l'interface dmz :

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



Remarque : Sur l'interface dmz, vous devez filtrer avec le protocole GRE. Le paquet de redirection est encapsulé dans le paquet GRE vers le client wccp.

Étape 3 : Débogage pour wccp

Exécutez les commandes suivantes :

debug wccp event debu wccp packet

Le bogue Cisco [IDCSCvn90518](#) a été soulevé pour amélioration afin d'avoir la prise en charge du mode natif FDM et FMC pour la configuration WCCP.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.