WCCPv2

ARTICA v4.28.030301

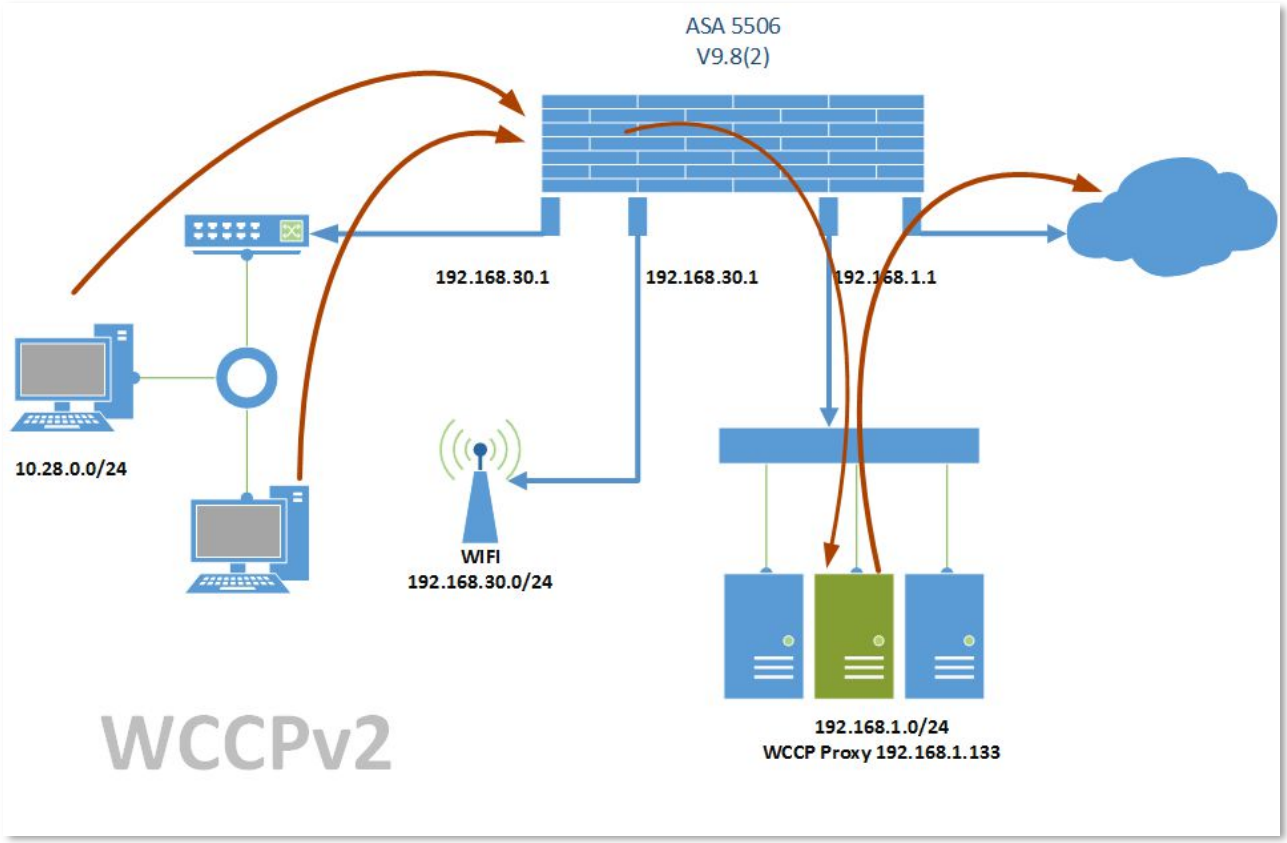
TABLE OF CONTENTS

INTRODUCTION

Web Cache Communication Protocol (WCCP) is a technology developed by Cisco that allows transparent re-direction of network traffic in real-time.
This re-direction can be to a cache engine or to a proxy, such as Artica Proxy.
In our example, we using CISCO ASA but you can use any "wccp-compatible router" such as Fortinet (Fortigate)

HOW IT WORKS

WCCP works by placing a WCCP capable router/switch in between users and the internet, either in the path or as the default gateway.
The WCCP device will then transparently redirect traffic on the ports that are configured over to the Artica Proxy for filtering and proxying.
The user has no idea that the "proxy" is in place as all traffic is sent from the proxy directly back to the user while spoofing the server's IP address



PREPARE THE CISCO ASA

Use the command-line utility in order to build ACLs for the CISCO ASA

THE CISCO LISTEN INTERFACE

We named our interface **DATACENTER** with the **192.168.1.1** network address.

```
interface GigabitEthernet1/3
 description DATACENTER INTERFACE
 nameif DATACENTER
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

DEFINE NETWORK OBJECTS

Our Artica Proxy server with WCCP enabled use **192.168.1.133** address

```
object network proxy133
 host 192.168.1.133
 description Server Artica WCCP ip 133
```

This group is able to store all WCCP Artica servers, if you need to add a second Artica proxy server with WCCP enabled, create a new object proxy134 for example and add it to this group.

```
object-group network wccp-artica
 description Artica servers using WCCP
 network-object object proxy133
```

This group is used to specify which "client"' networks will be redirected in HTTP/HTTPS, in our case, we redirect only the network that stores Artica itself

```
object-group network wccp-hooked
 description networks redirected by WCCP
 network-object 192.168.1.0 255.255.255.0
```

This group is used to deny the router to forward protocols using WCCP.
It is mandatory to first exclude Artica server itself in order to prevent looping.
Useful to whitelist some inside the wccp-hooked object

```
object-group network wccp-whitelist
 description IPs excluded from WCCP
 network-object object wccp-artica
```

ACCESS LISTS

Access list for HTTP traffic.

```
access-list wccp-traffic-http extended deny ip object-group wccp-whitelist any
access-list wccp-traffic-http extended permit ip object-group wccp-hooked any eq www
```

Same For the SSL protocol

```
access-list wccp-traffic-https extended deny ip object-group wccp-whitelist any
access-list wccp-traffic-https extended permit ip object-group wccp-hooked any eq
https
```

ENABLE THE WCCP FEATURE

Enable the WCCP traffic for HTTP protocol with the DATACENTER Interface for wccp-artica group

```
wccp web-cache redirect-list wccp-traffic-http group-list wccp-artica
wccp interface DATACENTER web-cache redirect in
```

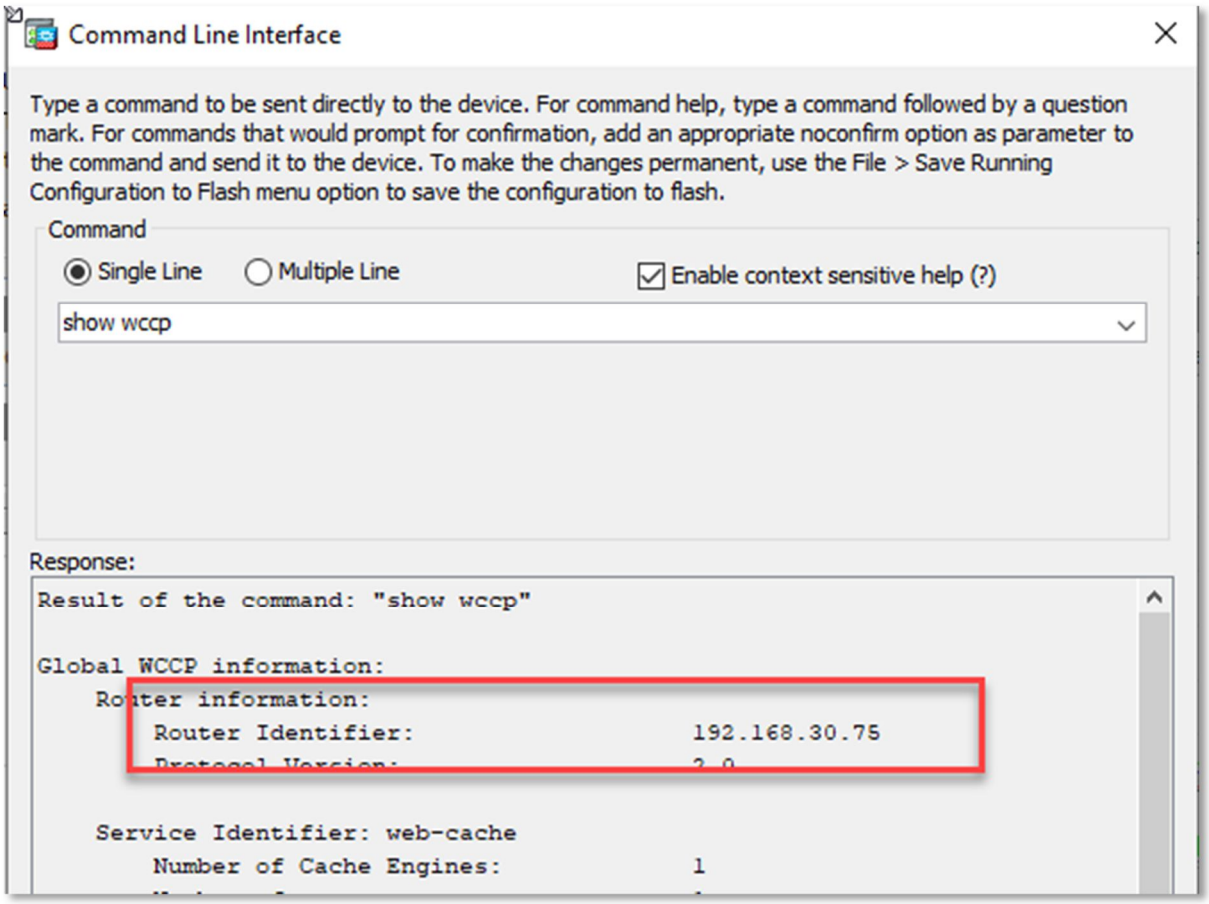
Enable the WCCP traffic for SSL protocol with the DATACENTER Interface for wccp-artica group

```
wccp 70 redirect-list wccp-traffic-https group-list wccp-artica
wccp interface DATACENTER 70 redirect in
```

After these 2 wccp rules, you CISCO ASA will try to communicate for all nodes stored by the **wccp-artica** group.

CHECKS THE ROUTER ID.

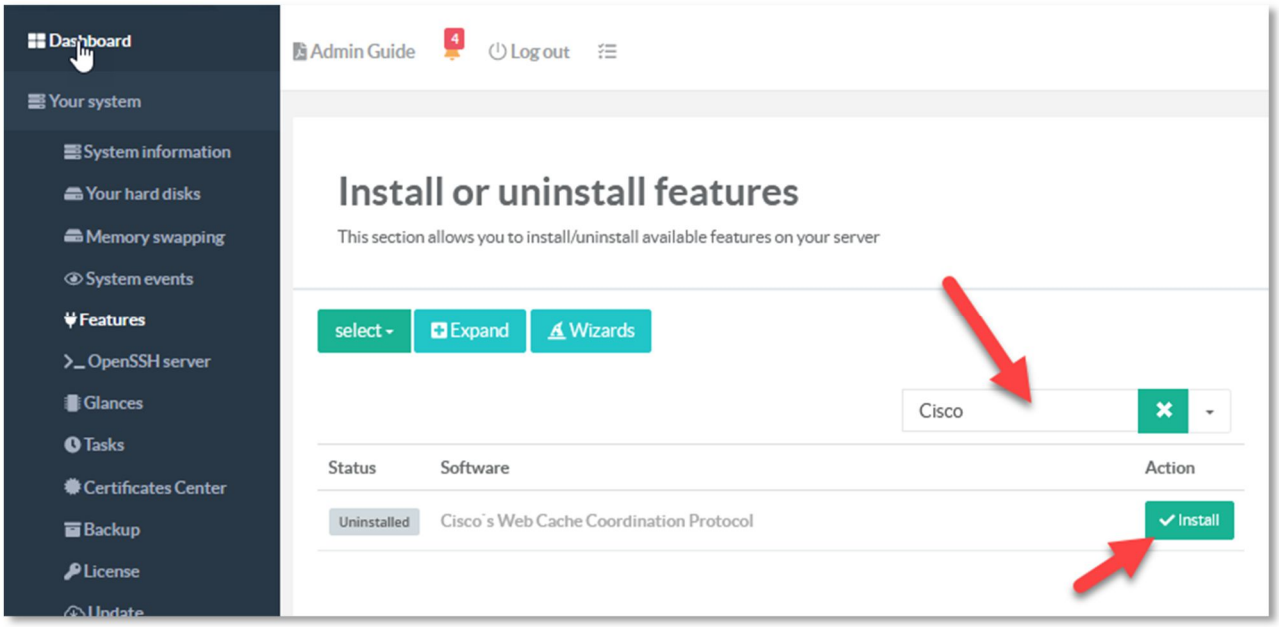
Type **show wccp** and check the "Router Identifier", It is an IP address automatically defined by the router.
Did not care about the network of the IP address, it is only used for the GRE connection.
It make no sense trying to modify it.



PREPARE YOUR ARTICA SERVER

INSTALL THE FEATURE

In the feature section, search the entry **Cisco** in the search field.
Under the **Cisco's Web Cache Coordinator Protocol**, click on "**Install**" button.

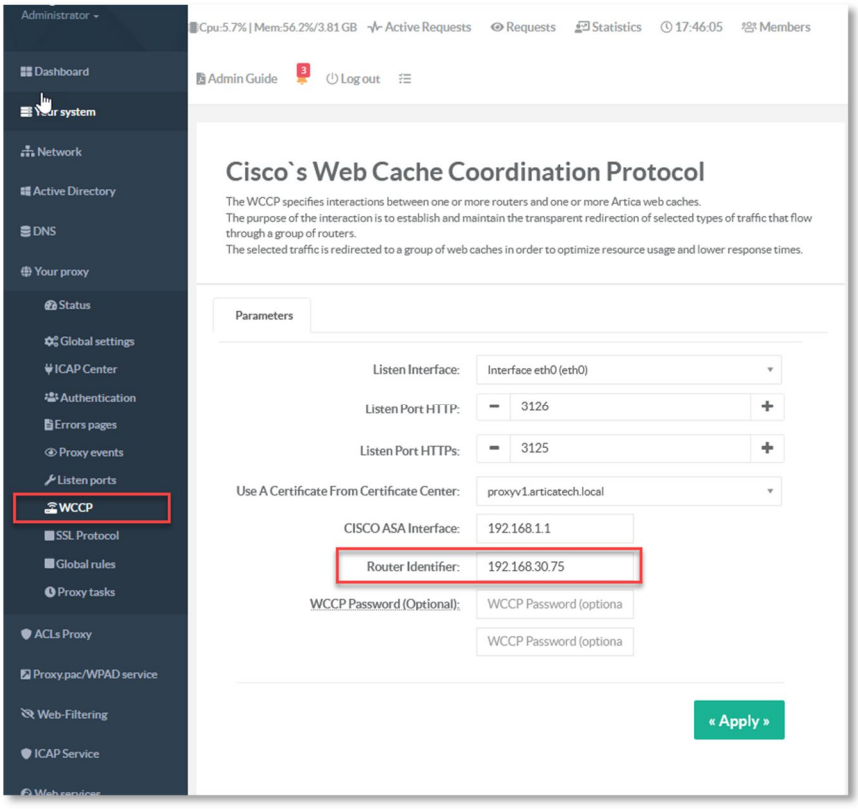


CONFIGURE YOUR ARTICA SERVER

On the left menu, choose "Your Proxy" and WCCP

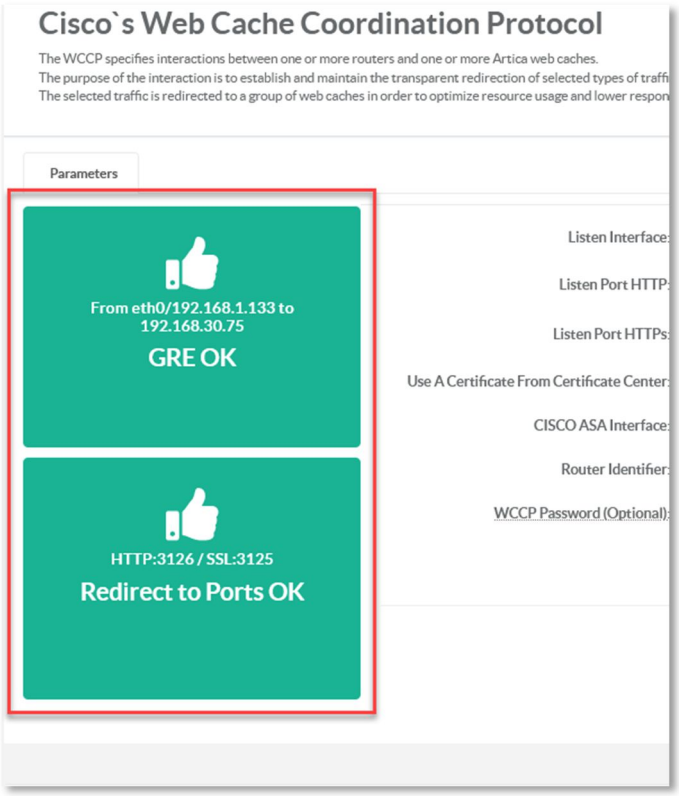
- Set the Interface that is able to communicate with the CISCO router under "Listen Interface" field
- Listen HTTP Port and HTTS port are the local ports used by the proxy. Defaults 3126 and 3125 are not used and you keep them in default mode.
- Select a certificate created by the certificate center feature in order to enable the SSL hook method.
- (Put a certificate did not mean that the proxy will decrypt the protocol). It is just mandatory.
- Set the IP address of the CISCO network interface that handle the Artica server network.
- Set the router identifier defined by the CISCO router when using the show wccp command line.

WCCP Password is optional, if you have defined



CHECK THE IMPLEMENTATION

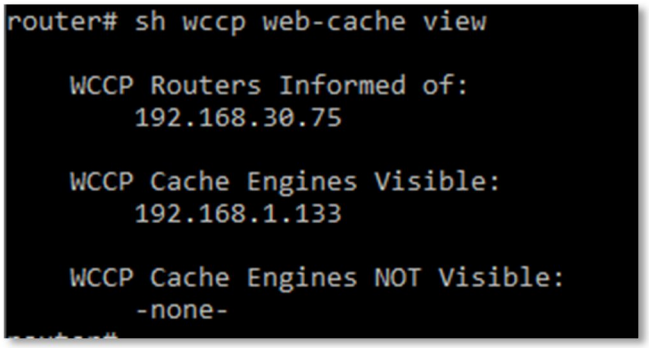
After apply settings, you should see green status of the GRE interface and the redirected ports



The command

```
sh wccp web-cache view
```

should display the IP address of your Artica server.



This means your router and your Artica server is linked and able to redirect HTTP/HTTPS protocols.

CISCO INFORMATIONS

WHY 70 NUMBER FOR DYNAMIC SERVICE ?

The table below displays the service ID and type of service. As you see we use HTTP (service 0) and HTTPS (service 70) for the proxy redirection.

Service Group	Type	Description
Service 0	Web-cache	Web caching service that permits the ASA to redirect HTTP traffic to the CE.
Service 53	DNS	DNS caching service that permits the ASA to redirect DNS client requests transparently to the client engine.
Service 60	FTP-native	Caching service that permits the ASA to redirect FTP native requests transparently to a single port on the content engine.
Service 70	https-cache	Caching service that permits the ASA to intercept port 443 TCP traffic and redirect this HTTPS traffic to the content engine.
Service 80	rtsp	Media streaming service that permits the ASA to redirect Real Time Streaming Protocol (RTSP) client requests to a single port on the content engine.
Service 81	mmst	Media caching service that permits the ASA to use TCP-based Microsoft Media Server (MMST) redirection in order to route Windows Media Technology (WMT) client requests to TCP port 1755 on the content engine.
Service 82	mmsu	Media caching service that permits the ASA to use User Datagram Protocol (UDP)-based Microsoft Media Server (MMSU) redirection in order to route WMT client requests to UDP port 1755 on the content engine.
Service 83	wmt-rtsp	Media streaming service that allows the ASA to redirect RTSP requests from Windows Media Service 9 clients to UDP port 5005 on the the CE.
Service 90-97	user configurable	User-defined WCCP services that support up to eight ports for each WCCP service. When you configure these user-defined services, you must specify whether to redirect the traffic to the HTTP caching application, to the HTTPS application, or to the streaming application on the content engine.
Service 98	custom-web-cache	Caching service that permits the ASA to transparently redirect HTTP traffic to the content engine on multiple ports other than port 80.
Service 99	reverse-proxy	Caching service that permits the ASA to redirect HTTP reverse proxy traffic to the content engine on port 80.

REMOVE WCCP CONFIGURATION:

To remove the entire WCCP configuration, type

```
clear configure wccp
```

DEBUG WCCP PACKETS

Open a telnet/SSH session on the router.

Type:

```
enable
debu wccp packets
term mon
```

You should see

```
WCCP-PKT:D70: Received valid Here_I_Am packet from 192.168.1.133 w/rcv_id 0000330C
WCCP-PKT:D70: Sending I_See_You packet to 192.168.1.133 w/ rcv_id 0000330D
WCCP-PKT:S00: Received valid Here_I_Am packet from 192.168.1.133 w/rcv_id 000032D5
WCCP-PKT:S00: Sending I_See_You packet to 192.168.1.133 w/ rcv_id 000032D6
WCCP-PKT:D70: Received valid Here_I_Am packet from 192.168.1.133 w/rcv_id 0000330D
WCCP-PKT:D70: Sending I_See_You packet to 192.168.1.133 w/ rcv_id 0000330E
WCCP-PKT:S00: Received valid Here_I_Am packet from 192.168.1.133 w/rcv_id 000032D6
WCCP-PKT:S00: Sending I_See_You packet to 192.168.1.133 w/ rcv_id 000032D7
```

To disable debug mode:

```
un all
```