How do I read or interpret the WCCP logs on Cisco Web Security appliance?

TAC   **Document ID: 118479**

Contributed by Josh Wolfer and Siddharth Rajpathak, Cisco TAC Engineers.

Oct 10, 2014

Contents

Question

How do I read or interpret the WCCP logs on Cisco Web Security appliance?

Environment

Cisco Web Security Appliance (WSA), all versions of AsyncOS

In AsyncOS version 7.1 and below: WCCP messages are logged in the Proxy Logs.

In AsynOS version 7.5 and above: WCCP messages is seen in WCCP logs along with the proxy logs.

Check your "Log Subscriptions" (under GUI > System Administration > Log Subscriptions) to make sure the proxy and/or WCCP logs are enabled.

In AsyncOS version 7.1 and below: The WCCP logging level can be changed by entering the following CLI command:

```
wsa01> advancedproxyconfig
[]> wccp

Enter values for the various "wccp" options:

Enter the log level for debugging WCCP :
[0]> 3
```

On AsyncOS version 7.5 and above: The logging level for WCCP logs and/or proxy logs can be changed in GUI under $"$System Administration $>$ Log Subscriptions $> <Corresponding-WCCP-Log-Name>"$

The logging levels will show the following data:

7.1 log level (CLI)	7.5 Log level (GUI)	Information seen in logs at the configured log level
0	Critical	Errors

1	Warning	Errors, CONFIG,
2	Information	Errors, CONFIG, INFO
3	Debug	Errors, CONFIG, INFO, STATE
4	Trace	Errors, CONFIG, INFO, STATE, CHANGE (state changes)

The logs can be broken into a few different areas *(separated by space indentation)* after the CONFIG is printed:

Timestamp
SVC   : Service ID data
Nexus : Nexus data – For each service, for each router, there is one nexus *(Can be thought as a virtual basket where data is kept)*
Rtr   : Router data
WC   : Web cache data

The following below is an explanation of the possible values you can find in the WCCP trace logging level. The exact example below is from a real scenario.

```
wccp: CONFIG:SG:0: type 0
wccp: CONFIG:SG:0: 80
wccp: CONFIG:0:[raptor]
wccp: CONFIG:0: GRE & L2
wccp: CONFIG:0:ret GRE & L2
wccp: CONFIG:0:TCP
wccp: CONFIG:0: 172.28.15.33
wccp: CONFIG:SG:0: Security enable <- 1
wccp: CONFIG:SG:0: Hash enable <- 1
wccp: CONFIG:SG:0: Mask enable <- 1
wccp: CONFIG:SG:0: Service direction <- 0
wccp: CONFIG:SG:0: Hash/mask on client <- 0
wccp: INFO:WCCPv2: local IP is 10.251.0.73
wccp: INFO:Accepting WCCP messages on port 2048, FD 3 at 10.251.0.73.
wccp: INFO:Openning a socket set
```

WCCP Configuration Information

```
wccp: INFO:### Timestamp 100 ###
```

*The **timestamp** always start at 100. This value increments in seconds.*

Service (SVC) Data

```
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
```
SVC: Service @<<memory pointer – for developement debugging>>
 Index: Position of this service in the list of all configured services on the WSA – Starts at 0 and increments +1
 *Type: 0 = Pre–defined ID (such as **web–cache**). 1 = Standard ID*
   Currently web–cache (service ID 0) is the only existing pre–defined ID
 ID: Service ID number (0 – 255)

```
wccp: STATE:     [MD5][MH_UNDECIDED][HASH_OK][MASK_OK][HASHING]
                 [L2FWD_OK][GREFWD_OK][LGR_UNDECIDED][L2RET_OK]
                 [GRERET_OK][RET_GRE][DWC_UNKNOWN][FWD][SERVER]
```

[MH_UNDECIDED] Load balancing method is undetermined at this time (hashing vs. masking)
[HASH_OK] Hashing is allowed
[MASK_OK] Masking is allowed
[HASHING] Hashing is the chosen method
[MASKING] Masking is the chosen method
[MH_DONE] Masking / hashing negotiation is complete

[L2FWD_OK] L2 for forward redirection is allowed
[GREFWD_OK] GRE for forward redirection is allowed

[LGR_UNDECIDED] Return redirection method is undetermined at this time (L2 vs. GRE)
[L2RET_OK] L2 for return redirection method is allowed
[GRERET_OK] GRE for return redirection method is allowed
[RET_GRE] GRE for Return method is preferred
[LGR_DONE] GRE / L2 return method negotion is complete

[DWC_UNKNOWN] Designated Web Cache (DWC) is unknown at this time
[FWD] Redirection is based on destination port
*[SERVER] Hashing / masking is based on the **server** address*
*[CLIENT] Hashing / masking is based on the **client** address*

[VIEW_CHANGED] The service view has changed

```
wccp: STATE:    needRA(=0)@0, ISY@0, viewchg=0, viewused=0, keychg=0
```

*NeedRA: Need Redirect Assign (**RA**). If **1** = Something in this service view has changed. If we are the **DWC**, we need to send a RA.*

- *Only the DWC sends RAs − at this point we don't know if we are the DWC)*
- *@0: The timestamp scheduled to send the RA in the future. (If this value were 115, the RA would be sent in 15 seconds)*

ISY@: The timestamp of the last received "I See You (ISY)" for this service.
Viewchg: The number of times this service has had any change (routers join / leave, wc added / removed, so forth)
Viewused: The last change number that we notified the router of.
Keychg: Number of times we have generated a different hash / mask table to send out

```
wccp: STATE:    this period:(HIAs=0, ISYs=0) proto=6
```

This period: In the last 10 seconds (standard tick), how many:
  HIA: "Here I Am (HIA)" packets we've sent
  ISY: "I See You (ISY)" packets we've received
*Proto: Protocol this service is asking to redirect. 6 is **TCP***

```
wccp: STATE:    ports = 0, 0, 0, 0, 0, 0, 0, 0
```

Ports: Ports to be redirected to the web cache (WC). When using web−cache the ports are left blank, but port 80 will be redirected.

Nexus Data

```
wccp: STATE:    nexus@0x0x85bf000: rcvd_key(0.0.0.0,0) sent_key(0.0.0.0,0)
```

Nexus: For each service, for each router, there is one nexus (Can be thought as a virtual basket where data is kept)

Recvd_key: Address of the DWC that sent the RA, the keychg number the DWC sent (incremental)
  Sent_key: Our address + key_chg number when we were the DWC

```
wccp: STATE:     rtr_mention@0, ISY@0 rtr_change#= 0 refs=0
```

Rtr_mention: Router last mentioned itself @ <timestamp>
ISY: Last saw an ISY from this router in this service group @<timestamp> (nexus router)
Rtr_changer#: Number of times the router believes the view has changed

```
wccp: STATE:     [FIXED][DEAD][FWD_???]
```

These are flags for this nexus
 [FIXED]: Router is configured to be used
 [DEAD]: Router Not responding / haven't used it yet
 [ALIVE]: Router has responded with an ISY
 [FWD_xxx]: Agreed upon forwarding redirection method (L2 / GRE)
 [NEG_PEND]: WCCP negotiation is pending
 [ACTIVE]: WCCP negotiation is complete and WCCP is 'Active'
 [VIEW_VALID]: WCCP negotiation is complete and WSA + router agree on capabilitues

```
wccp: STATE:     rstate=0, outst_HIA=0, receiveID=0
```

Rstate: ??
 Outst_HIA: Number of HIAs we have sent, but not received an ISY to. After getting an ISY, this resets to 0.
 ReceiveID: Receive ID increments on each successful ISY.

Router Data

```
wccp: STATE:  rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
```

Rtr: Router information for this nexus – duplicated for nexii on the same router
 Fd: File descriptor of the socket to send packets to this router
 Gre: Number of the GRE interface that we should receive data from this router (gre0, gre1,...)
 Bind: Address that we are binding our socket to, to send packets to this router (Our from / source address)
 Sentto: Address the router is reporting that it got packets to that were sent from us (only useful when using multicast)

```
wccp: STATE:     configaddr=172.28.15.33, ID_addr=0.0.0.0, from_addr=172.28.15.33
```

Configaddr: IP address for the router that is configured
 ID_addr: Advertized router identifier address
 From_addr: Address where the packets really came from (source IP)

Web cache data

```
wccp: STATE:  WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
```

<IP> mentioned: The IP of the referenced WC and the timestamp it was introduced into the service ID
Weight: Metric shared among WCs to share load data.
Status: ??

```
wccp: STATE:    [ME][ACTIVE]
```

[ME]: This WC is the WSA were running this daemon
[ACTIVE]: The WC has been reported by ALL routers in this service

Below is a complete sample output and break down of a WCCP level 3 log. In this log, the WSA is joining a service ID that has 2 other WSAs already in it. The WSA will become the DWC (since it has the lowest IP in the service):

```
wccp: INFO:### Timestamp 100 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:    [MD5][MH_UNDECIDED][HASH_OK][MASK_OK][HASHING]
       [L2FWD_OK][GREFWD_OK][LGR_UNDECIDED][L2RET_OK]
       [GRERET_OK][RET_GRE][DWC_UNKNOWN][FWD][SERVER]
wccp: STATE:    needRA(=0)@0, ISY@0, viewchg=0, viewused=0, keychg=0
wccp: STATE:    this period:(HIAs=0, ISYs=0) proto=6
wccp: STATE:    ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:  nexus@0x0x85bf000: rcvd_key(0.0.0.0,0) sent_key(0.0.0.0,0)
wccp: STATE:    rtr_mention@0, ISY@0 rtr_change#= 0 refs=0
wccp: STATE:    [FIXED][DEAD][FWD_???]
wccp: STATE:    rstate=0, outst_HIA=0, receiveID=0
wccp: STATE:  rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:    configaddr=172.28.15.33, ID_addr=0.0.0.0, from_addr=172.28.15.33
```

Nothing has been sent out yet – all initialization data.

```
wccp: INFO:### Timestamp 101 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:    [MD5][MH_UNDECIDED][HASH_OK][MASK_OK][HASHING]
       [L2FWD_OK][GREFWD_OK][LGR_UNDECIDED][L2RET_OK]
       [GRERET_OK][RET_GRE][DWC_UNKNOWN][FWD][SERVER]
wccp: STATE:    needRA(=0)@0, ISY@0, viewchg=0, viewused=0, keychg=0
wccp: STATE:    this period:(HIAs=0, ISYs=0) proto=6
wccp: STATE:    ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:  nexus@0x0x85bf000: rcvd_key(0.0.0.0,0) sent_key(0.0.0.0,0)
wccp: STATE:    rtr_mention@0, ISY@0 rtr_change#= 0 refs=0
wccp: STATE:    [FIXED][DEAD][FWD_???]
wccp: STATE:    rstate=0, outst_HIA=0, receiveID=0
wccp: STATE:  rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:    configaddr=172.28.15.33, ID_addr=0.0.0.0, from_addr=172.28.15.33
wccp: INFO:send_HIA called
wccp: INFO:### Timestamp 101 ###
wccp: INFO:HIA sent to 172.28.15.33  -- 1 ISY(s) outstanding
wccp: INFO:### Timestamp 101 ###
wccp: INFO:ISY received from 172.28.3.46.(708 bytes)
wccp: INFO:ISY: accepted
```

We sent out the first HIA @ 101 and received back an ISY @101. Below is the update of the view now that we've received an ISY.

```
wccp: INFO:### Timestamp 101 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
```

```
wccp: STATE:     [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
                     [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
                     [DWC_UNKNOWN][VIEW_CHANGED][FWD][SERVER]
wccp: STATE:     needRA(=0)@0, ISY@101, viewchg=1, viewused=0, keychg=0
wccp: STATE:     this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:     ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:  WC@0x0x85b9160: (172.17.0.10) mentioned:101 weight:1 status:0
wccp: STATE:     [ACTIVE]
wccp: STATE:  WC@0x0x85b9140: (172.28.6.34) mentioned:101 weight:1 status:0
wccp: STATE:     [ACTIVE]
wccp: STATE:  nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE:     rtr_mention@101, ISY@101 rtr_change#= 23 refs=0
wccp: STATE:     [FIXED][ALIVE][ACTIVE][NEG_PEND][FWD_???][FWD_GRE]
                     [VIEW_VALID]
wccp: STATE:     rstate=0, outst_HIA=0, receiveID=158
wccp: STATE:  rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:     configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.15.33
```

We recognize the other 2 web caches and they are flagged ACTIVE. The current DWC is 172.17.0.10 per the rcvd_key in the nexus. Nexus status is NEG_PEND, ReceiveID=158.

```
wccp: INFO:### Timestamp 111 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:     [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
                     [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
                     [DWC_UNKNOWN][FWD][SERVER]
wccp: STATE:     needRA(=1)@117, ISY@101, viewchg=1, viewused=0, keychg=0
wccp: STATE:     this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:     ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:  WC@0x0x85b9160: (172.17.0.10) mentioned:101 weight:1 status:0
wccp: STATE:     [ACTIVE]
wccp: STATE:  WC@0x0x85b9140: (172.28.6.34) mentioned:101 weight:1 status:0
wccp: STATE:     [ACTIVE]
wccp: STATE:  nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE:     rtr_mention@101, ISY@101 rtr_change#= 23 refs=0
wccp: STATE:     [FIXED][ALIVE][ACTIVE][NEG_PEND][FWD_???][FWD_GRE]
                     [VIEW_VALID]
wccp: STATE:     rstate=0, outst_HIA=0, receiveID=158
wccp: STATE:  rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:     configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.15.33
wccp: INFO:send_HIA called
wccp: INFO:### Timestamp 111 ###
wccp: INFO:HIA sent to 172.28.15.33  -- 1 ISY(s) outstanding
wccp: INFO:### Timestamp 111 ###
wccp: INFO:ISY received from 172.28.3.46.(1252 bytes)
wccp: INFO:ISY: accepted
```

Since the service view has changed, needRA is flagged. Expecting an RA @117. Also note that the router change # is 23. You'll see that we sent out another HIA at 111 and received another ISY at 111.

```
wccp: INFO:### Timestamp 111 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:     [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
                     [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
                     [DWC_UNKNOWN][VIEW_CHANGED][FWD][SERVER]
wccp: STATE:     needRA(=1)@117, ISY@111, viewchg=2, viewused=0, keychg=0
wccp: STATE:     this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:     ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:  WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
wccp: STATE:     [ME][ACTIVE]
wccp: STATE:  WC@0x0x85b9160: (172.17.0.10) mentioned:111 weight:1 status:0
```

```
wccp: STATE:    [ACTIVE]
wccp: STATE:  WC@0x0x85b9140: (172.28.6.34) mentioned:111 weight:1 status:0
wccp: STATE:    [ACTIVE]
wccp: STATE:  nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE:    rtr_mention@111, ISY@111 rtr_change#= 24 refs=0
wccp: STATE:    [FIXED][ALIVE][ACTIVE][FWD_GRE]
wccp: STATE:    rstate=0, outst_HIA=0, receiveID=161
wccp: STATE:  rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:    configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.3.46
```

The view has changed again and the viewchg is incremented accordingly. The router also noticed a change and incremented its change #. You'll see that THIS WSA is now being reported and labeled ACTIVE. This means that all the routers on this service have mentioned the WC.

```
wccp: INFO:### Timestamp 117 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:    [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
                    [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
                    [DWC][FWD][SERVER]
wccp: STATE:    needRA(=1)@117, ISY@111, viewchg=2, viewused=0, keychg=0
wccp: STATE:    this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:    ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:  WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
wccp: STATE:    [ME][ACTIVE]
wccp: STATE:  WC@0x0x85b9160: (172.17.0.10) mentioned:111 weight:1 status:0
wccp: STATE:    [ACTIVE]
wccp: STATE:  WC@0x0x85b9140: (172.28.6.34) mentioned:111 weight:1 status:0
wccp: STATE:    [ACTIVE]
wccp: STATE:  nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE:    rtr_mention@111, ISY@111 rtr_change#= 24 refs=0
wccp: STATE:    [FIXED][ALIVE][ACTIVE][FWD_GRE]
wccp: STATE:    rstate=0, outst_HIA=0, receiveID=161
wccp: STATE:  rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:    configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.3.46
wccp: INFO:send_RA: called.
wccp: INFO:initial mask is 0x00000000
wccp: INFO:slots = 32 WCs = 3, mask = 0x00000526, inc = 0x2
wccp: INFO:slot 0,val 0x00000000, index - 0
wccp: INFO:slot 1,val 0x00000002, index - 1
wccp: INFO:slot 2,val 0x00000004, index - 2
wccp: INFO:slot 3,val 0x00000006, index - 0
wccp: INFO:slot 4,val 0x00000020, index - 1
wccp: INFO:slot 5,val 0x00000022, index - 2
wccp: INFO:slot 6,val 0x00000024, index - 0
wccp: INFO:slot 7,val 0x00000026, index - 1
wccp: INFO:slot 8,val 0x00000100, index - 2
wccp: INFO:slot 9,val 0x00000102, index - 0
wccp: INFO:slot 10,val 0x00000104, index - 1
wccp: INFO:slot 11,val 0x00000106, index - 2
wccp: INFO:slot 12,val 0x00000120, index - 0
wccp: INFO:slot 13,val 0x00000122, index - 1
wccp: INFO:slot 14,val 0x00000124, index - 2
wccp: INFO:slot 15,val 0x00000126, index - 0
wccp: INFO:slot 16,val 0x00000400, index - 1
wccp: INFO:slot 17,val 0x00000402, index - 2
wccp: INFO:slot 18,val 0x00000404, index - 0
wccp: INFO:slot 19,val 0x00000406, index - 1
wccp: INFO:slot 20,val 0x00000420, index - 2
wccp: INFO:slot 21,val 0x00000422, index - 0
wccp: INFO:slot 22,val 0x00000424, index - 1
wccp: INFO:slot 23,val 0x00000426, index - 2
wccp: INFO:slot 24,val 0x00000500, index - 0
wccp: INFO:slot 25,val 0x00000502, index - 1
wccp: INFO:slot 26,val 0x00000504, index - 2
```

```
wccp: INFO:slot 27,val 0x00000506, index - 0
wccp: INFO:slot 28,val 0x00000520, index - 1
wccp: INFO:slot 29,val 0x00000522, index - 2
wccp: INFO:slot 30,val 0x00000524, index - 0
wccp: INFO:slot 31,val 0x00000526, index - 1
wccp: INFO:### Timestamp 117 ###
wccp: INFO:RA (mask) sent to 172.28.15.33.(624 bytes)
```

It's 117 now, the time specified for needing to send an RA. Now that this WSA is ACTIVE, we've decided that we are the DWC, since we are the lowest IP among the WCs. The INFO states that we need to send an RA. The load balancing method we've negotiated is MASKING. The Masking table uses a round robin index and is displayed. The INFO at the bottom shows that we have sent an RA @ 117.

```
wccp: INFO:### Timestamp 121 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:    [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
                [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
                [DWC][FWD][SERVER]
wccp: STATE:    needRA(=2)@127, ISY@111, viewchg=2, viewused=2, keychg=1
wccp: STATE:    this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:    ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE: WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
wccp: STATE:    [ME][ACTIVE]
wccp: STATE: WC@0x0x85b9160: (172.17.0.10) mentioned:111 weight:1 status:0
wccp: STATE:    [ACTIVE]
wccp: STATE: WC@0x0x85b9140: (172.28.6.34) mentioned:111 weight:1 status:0
wccp: STATE:    [ACTIVE]
wccp: STATE: nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(10.251.0.73,1)
wccp: STATE:    rtr_mention@111, ISY@111 rtr_change#= 24 refs=0
wccp: STATE:    [FIXED][ALIVE][ACTIVE][FWD_GRE][VIEW_VALID]
wccp: STATE:    rstate=0, outst_HIA=0, receiveID=161
wccp: STATE: rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:    configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.3.46
wccp: INFO:send_HIA called
```

The view is now valid and we've sent 1 redirect assign, as notified by the *sent_key*. At this point everything should be up and running and good.