

Verifying and Troubleshooting the Deployment

This chapter provides an overview of some of the verification and troubleshooting tools that can be used to complete the verification and any troubleshooting of the proxy deployment. It also provides a basic overview of some of the items on the Cisco WSA, infrastructure devices, and Windows Operations Systems to assist in basic verification and troubleshooting. However, it does not specifically prescribe action items as a result of the troubleshooting steps due to the fluidity of the deployment and potential architectural differences.

There are several methods of verifying and troubleshooting the deployment of the proxy and the associated redirection services in the infrastructure.

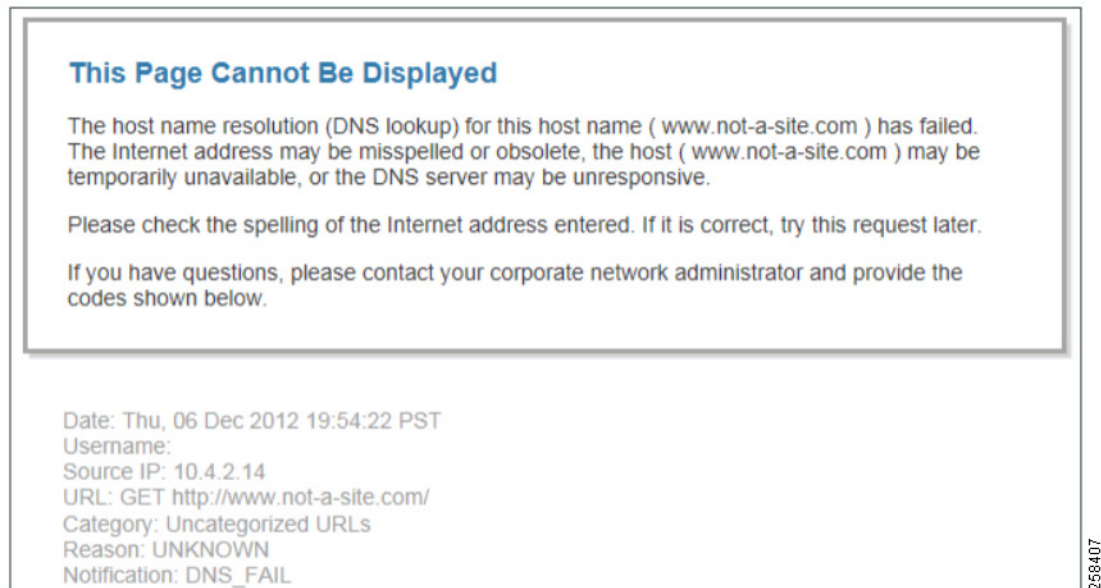
Web Browser Verification

Verification of the functionality of WCCP and the Cisco WSA can occur within the web browser itself by testing some addresses that may or may not be blocked depending on the configuration of the Cisco WSA:

- One address should be resolvable externally on the internet, for instance www.rockwellautomation.com, which should return without issue. This proves the client has internet access but does not prove the connection is going through Cisco WSA.
- The other address should be something not resolvable externally or something that may have been configured to be blocked. This request should return an error from the Cisco WSA, not the browser; proving that Cisco WSA is serving the content.

The Cisco WSA returns an error like that shown in [Figure 4-1](#).

Figure 4-1 Cisco WSA Error

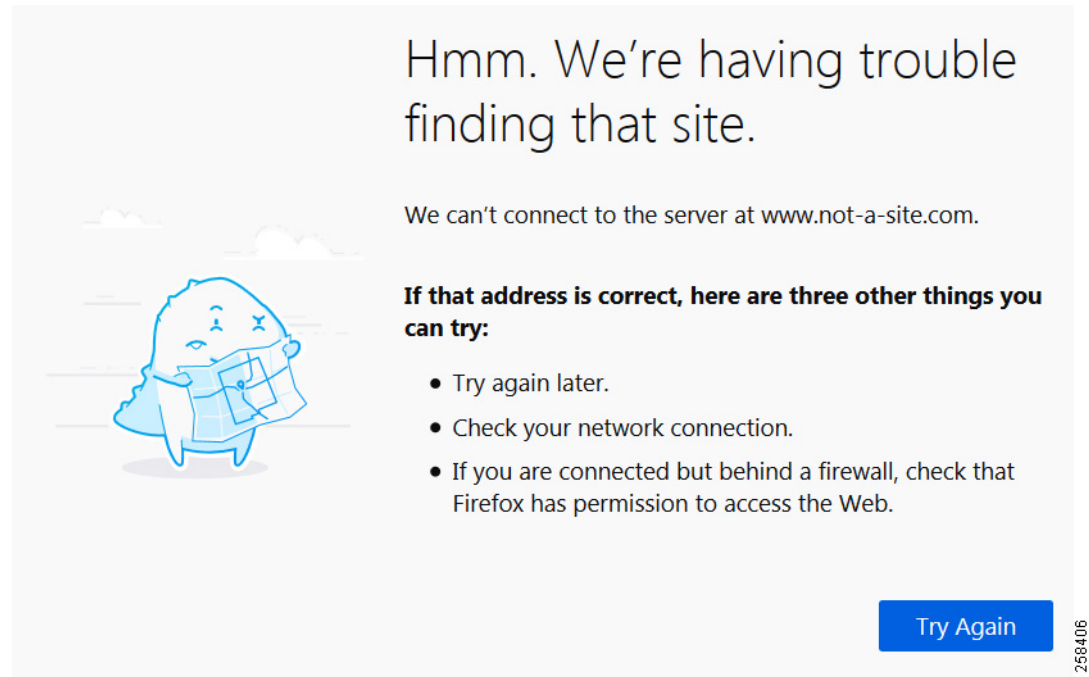


Some important items to note from the above error:

- URL—This is the website that was requested.
- Category—If the website is known and classified into one of the Cisco WSAs categories, this would be shown here. This is a good tool to determine which categories to allow or block if web sites are not working as expected. In this case, the requested URL is not categorized.
- Reason—This is the reason that the webpage is being blocked.
- Notification—This is a summary of the error shown to the user.

If the web request is not directed by the Cisco WSA, the web browser returns an error. An example with the Firefox browser returns an error similar to what is shown in [Figure 4-2](#).

Figure 4-2 FireFox Connection Error

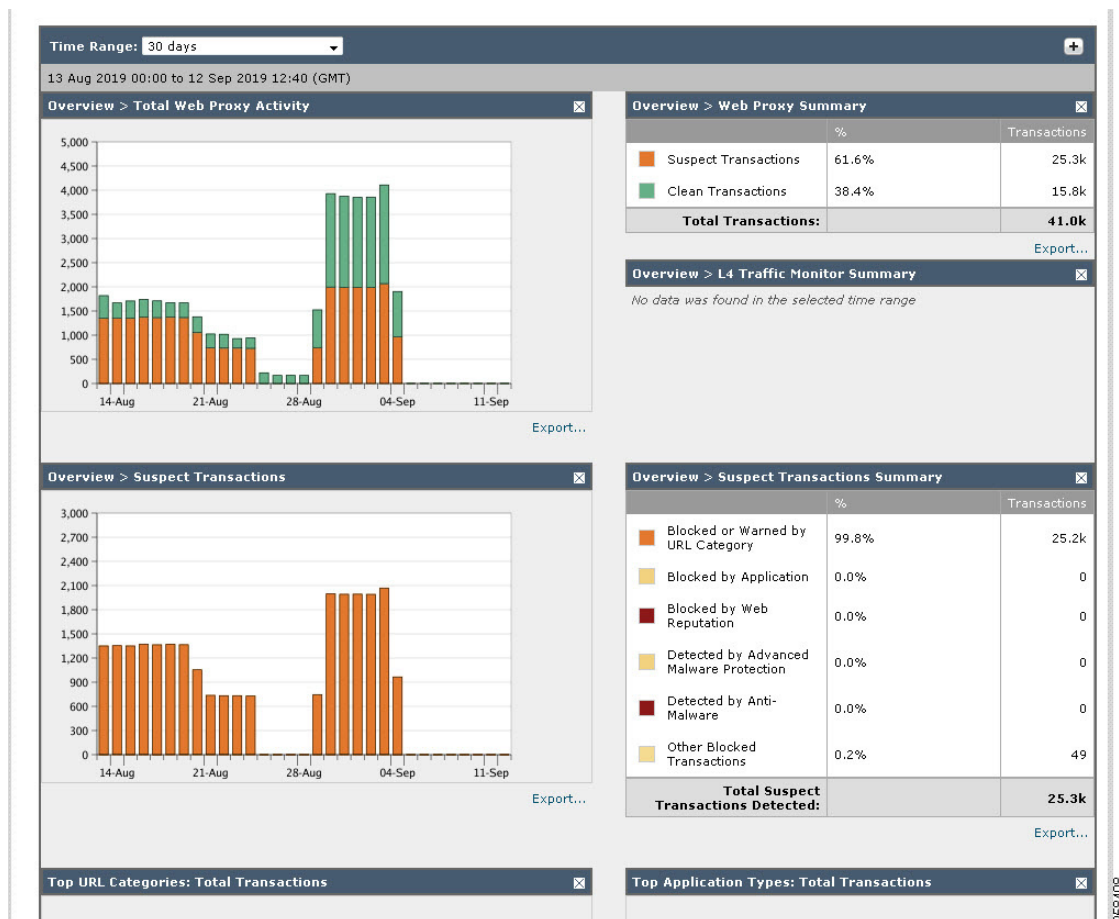


Cisco WSA Tools

From the home page of the Cisco WSA, there are several reporting tools that are available for verification, log management, and troubleshooting. These tools can be used to verify if the deployment of the Cisco WSA was successful. The Cisco WSA inspects all traffic that is forwarded to it and organizes it into two categories, Suspect Transactions and Clean Transactions. Based on the configuration of the Cisco WSA and overall usage, the ratios of Suspect to Clean may vary.

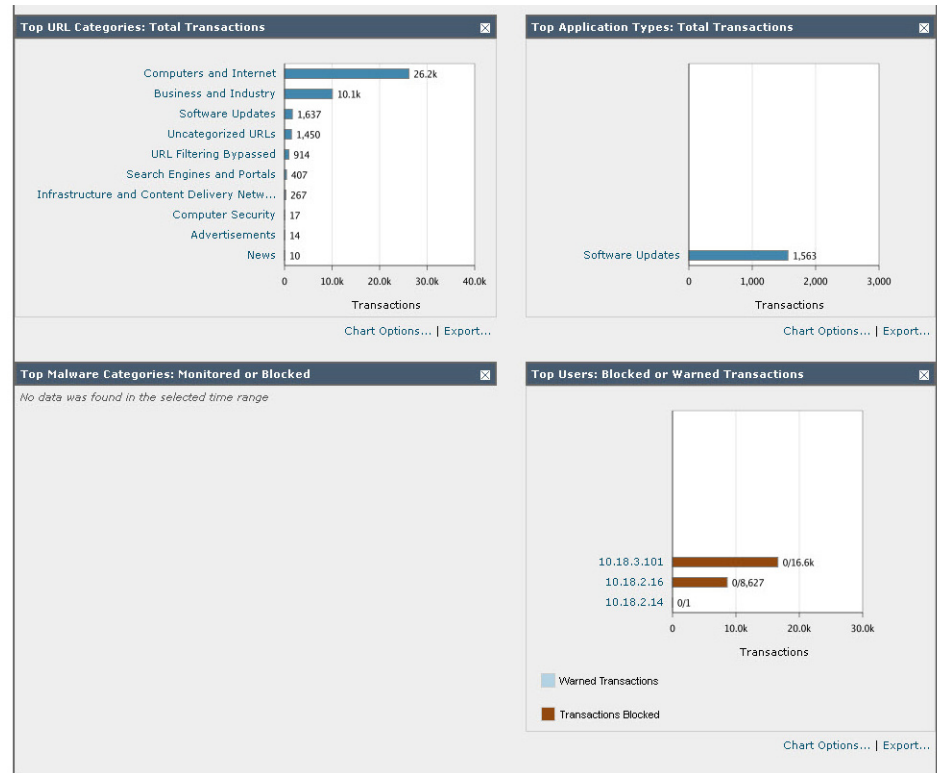
Figure 4-3 shows the reporting details from the Cisco WSA home page detailing the summary of traffic and the details of the Suspect Transactions.

Figure 4-3 Web Proxy Reporting



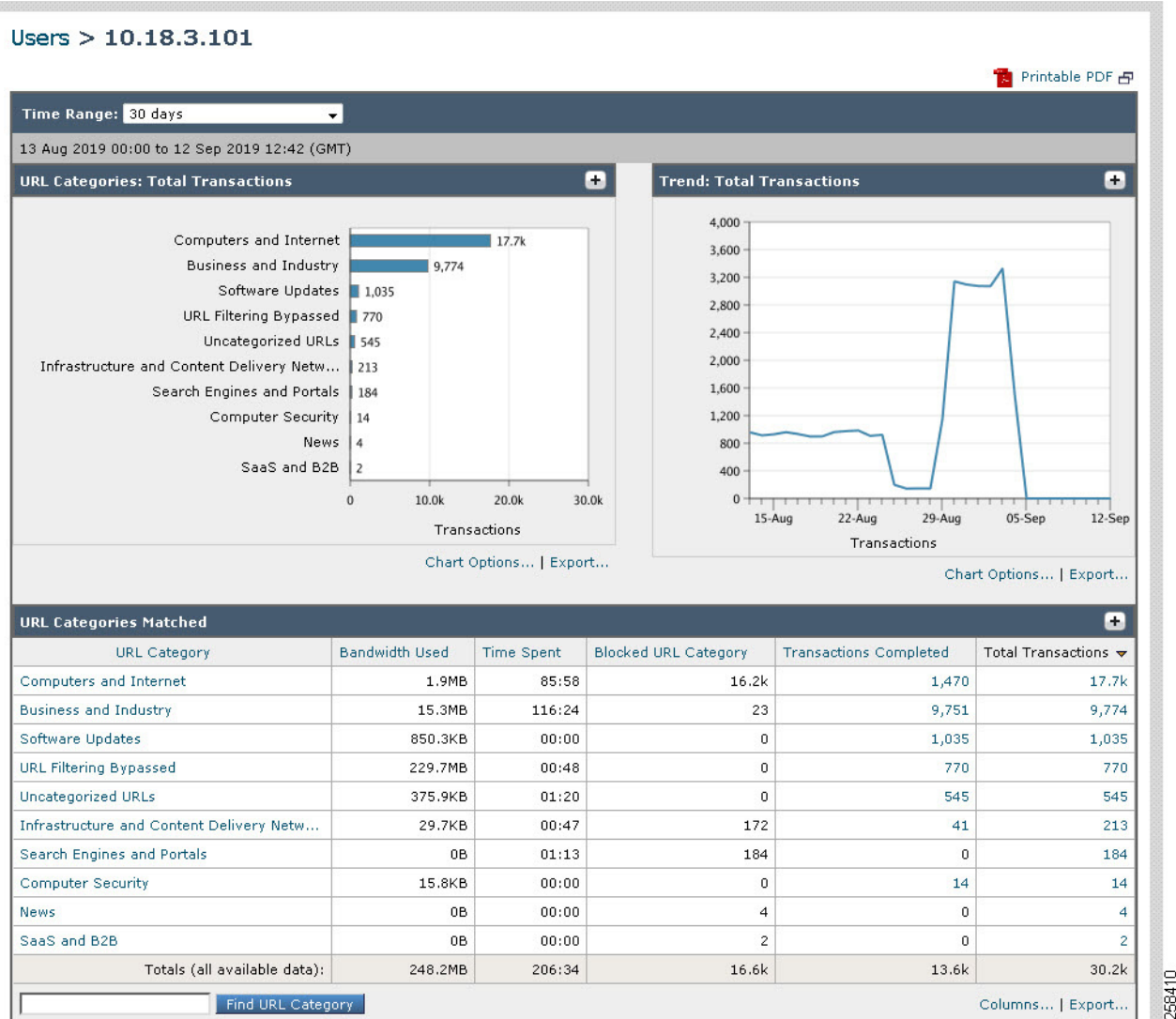
Additional information is shown in the lower half of the home page of the Cisco WSA. This information provides a more granular overview of the top URL categories as well as the top users as shown in Figure 4-4.

Figure 4-4 URL and User Reporting



These reporting options and top application types contain hyperlinks that provide more details. For example, clicking the IP address 10.18.3.101 under the top users section would provide additional information (Figure 4-5). Additional granularity is provided for each user, such as the amount of bandwidth and time spent in each of the URL categories.

Figure 4-5 User Report



Similar to the previous page, this report on user 10.18.3.101 has additional hyperlinks that can provide more details about the content the user is viewing. In [Figure 4-5](#), clicking one of the numbers in the transactions completed column will provide the URLs that were accessed by the user under each individual URL category.

[Figure 4-6](#) shows the breakdown of the URLs that have been accessed by the user. Additional information, such as full URL, content type, destination IP address, and Cisco WSA independent tracking can be accessed by clicking the individual URLs.

Figure 4-6 User URL Reporting

Generated: 12 Sep 2019 12:44 (GMT) Printable Download

Results					
			Items Displayed 50		
Displaying 1 - 50 of over 1000 items.			« Previous 1 2 3 ... 18 19 20 Next »		
Time (GMT +00:00) ▼	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
04 Sep 2019 11:39:03	https://api.rockwellautomation.com:443		Allow	860B	10.18.3.101
04 Sep 2019 11:38:02	https://api.rockwellautomation.com:443		Allow	860B	10.18.3.101
04 Sep 2019 11:37:02	https://api.rockwellautomation.com:443		Allow	860B	10.18.3.101
04 Sep 2019 11:36:01	https://api.rockwellautomation.com:443		Allow	860B	10.18.3.101
04 Sep 2019 11:35:00	https://api.rockwellautomation.com:443		Allow	860B	10.18.3.101
04 Sep 2019 11:34:00	https://api.rockwellautomation.com:443		Allow	858B	10.18.3.101
04 Sep 2019 11:32:59	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:31:58	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:30:57	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:29:57	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:28:56	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:27:55	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:26:54	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:25:54	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:24:53	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:24:21	https://www.ab.com:443 (2)		Allow	846B	10.18.3.101
04 Sep 2019 11:23:52	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:22:52	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:21:51	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:20:50	https://api.rockwellautomation.com:443		Allow	859B	10.18.3.101
04 Sep 2019 11:19:48	https://api.rockwellautomation.com:443 (3)		Allow	2,989B	10.18.3.101
04 Sep 2019 11:18:48	https://api.rockwellautomation.com:443		Allow	860B	10.18.3.101
04 Sep 2019 11:17:47	https://api.rockwellautomation.com:443		Allow	860B	10.18.3.101

There are many filtering options offered in the reporting and web tracking pages of the Cisco WSA to fine-tune and search specific URLs, actions, file sizes, etc.

Cisco CLI Verification and Troubleshooting

Since most WCCP deployment will rely on Layer 2 redirection, a good first step in troubleshooting deployment issues is to ensure that the WCCP device is able to ping the Cisco WSA. Additionally, using debug tools for WCCP is uninstrutive about the performance of the device due to the low number of messages that are generated. In addition to general debugging, the **show** commands can provide helpful information about the state of the deployment and the status of the current redirection service ID.



Note

Some devices exclude the **ip** in the command. For example, the above command **show ip wccp** is valid on a Catalyst 4500X, but on the Cisco ASA 5525 the command is **sh wccp**.

Table 4-1 WCCP Debug and Detail Commands

Debug Command	Result
show ip wccp web-cache detail	Displays proxy server and WCCP router statistics for a particular service group.
show ip wccp <service ID> view	Displays service group information.
debug ip wccp events	Displays information about significant WCCP events.
debug ip wccp packets	Displays information about every WCCP packet received or sent by the router.

Examples of the debug types of messages you will see are shown below:

- WCCP-EVNT:D90: Here_I_Am packet from 10.19.1.37: authentication failure
 - This indicates that if authentication (a password) is used for the WCCP service, there is a mismatch between the WCCP device and the Cisco WSA configuration.
- After initial configuration, verification of the WCCP success is shown:
 - WCCP-PKT:D90: Sending I_See_You packet to 10.18.3.37 w/ rcv_id 00000001
 - WCCP-EVNT: Adding NP rule to exclude WCCP redirection of web cache 10.18.3.37
 - WCCP-PKT:D90: Received valid Here_I_Am packet from 10.18.3.37 w/rcv_id 00000001
 - WCCP-EVNT:D90: Built new router view: 1 routers, 1 usable web caches, change # 00000002
 - WCCP-PKT:D90: Sending I_See_You packet to 10.18.3.37 w/ rcv_id 00000002

Table 4-2 Device Commands

Command	Result
show ip wccp	Displays global WCCP statistics.
show ip wccp <service ID>	Displays information about all known proxies.
show ip interface	Displays whether web cache redirecting is enabled on an interface.
show ip wccp / show ip wccp <service ID>	Displays a count of the number of packets redirected.
clear ip wccp	Clears the counter displayed by the show ip wccp and show ip wccp web-caches.

Using the **sh wccp** command, general information regarding the WCCP service can be viewed:

```
device# sh wccp 90
```

Table 4-3 Global WCCP Information

Router information:		
Router identifier	10.100.2.254	Defines the address and the devices ID. If this does not list an IP address, the Cisco WSA and the device may not be able to communicate.
Protocol version	2.0	Defines the WCCP version.

Table 4-3 Global WCCP Information (continued)

Router information:		
Service Identifier	90	Defines the Service ID that is shared with the Cisco WSA.
Number of Cache Engines	1	Defines number of Proxies in the group.
Number of Routers	1	Defines how many other devices are redirecting.
Total Packets Redirected	40	Defines the amount of traffic WCCP has sent to the Cisco WSA.
Redirect access-list	WCCP_Redirect	Defines which access-list is used to determine adjacency.
Total Connections Denied Redirect	0	Define how many packets were blocked.
Total Packets Unassigned	0	Defines how many packets did not fit into a category.
Group access-list	-none-	Defines which traffic should be redirected.
Total Messages Denied to Group	0	Defines how many messages were not sent due to the group access-list.
Total Authentication Failures	4	Invalid password between device and Cisco WSA.
Total Bypassed Packets Received	0	Packets set to bypass redirection.

