Troubleshoot Cloud Lookup Errors and URL Filtering Issues

Contents

Introduction

Prerequisites

Requirements

- Components Used

Configure

How to Verify the Cloud Lookup Failures and Connectivity Issues

- Step 1. DNS Resolution
- Step 2. Port Connectivity
- Step 3. File Download Check
- Step 4. Restart SFDC
- Step 5. Restart Snort Instance
- Step 6. Restart CloudAgent Service
- Step 7. Perform Packet Capture
- Step 8. Open a New Terminal and Run Debug
- Step 9. Perform Tests

Conclusion

Introduction

This document describes the possible issues related with the URL filtering and cloud look up errors.

Prerequisites

The URL filtering feature on FireSIGHT Management Center allows you to write a condition in an access control rule in order to determine the traffic that traverses a network based on non-encrypted URL requests by the monitored hosts.

Before starting with the configuration part, it is important that you need to verify the URL filtering license availability and need to make sure that it has been properly installed and enabled on the FireSIGHT system. Add category and reputation-based URL conditions to the access control rules. However without a URL filtering license, you cannot apply the access control policy towards the managed devices.

Requirements

Cisco recommends that you have the knowledge of these topics:

- Knowledge of Firepower technology.
- Basic Knowledge of FireSIGHT Management Center (FMC).

Components Used

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.

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

- ASA FirePower modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) running software version starting from 5.3 , 5.4 and above
- ASA FirePower module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) running software version starting from 5.3, 5.4 , 6.0.0 and above
- All Cisco FirePower 7000 Series and Cisco FirePOyouR 8000 Series
- FS 750 , FS 1500 , FS 3500 , FireSIGHT Management Center FS2000, FS4000 or virtual appliance with all software versions.

Configure

Refer the following article to start with the initial configurations .

https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/117956-technote-sourc...

How to Verify the Cloud Lookup Failures and Connectivity Issues

Verify the cloud lookup errors using these scenario-based troubleshooting steps.

Step 1. DNS Resolution

The FireSIGHT Management Center communicates with the following servers while performing the cloud lookup process.

```
database.brightcloud.com
service.brightcloud.com
```

As a first prerequisite to manage this connection , you need to make sure that both the servers are allowed on the firewalls. If the connections are allowed, then verify it using the following **nslookup** command to confirm if the servers are able to resolve the names without any fail.

```
root@123:#nslookup service.brightcloud.com
root@123:#nslookup database.brightcloud.com
```

Step 2. Port Connectivity

Once after confirming the domain connectivity , you need to check the connectivity of these domains to the required ports.

The FireSIGHT Systems use ports 443/HTTPS and 80/HTTP in order to communicate with the cloud services. Verify the connectivity to port 80 and 443 using the telnet command. The URL database is downloaded with database.brightcloud.com at port 443, while the unknown URL queries are done with service.brigthcloud.com at port 80.

```
root@123:#telnet service.brightcloud.com 80
root@123:#telnet database.brightcloud.com 80
root@123:#telnet database.brightcloud.com 443
```

If the telnet communication is successful, one of the output looks like this:

```
Connected to service.brightcloud.com.
Escape character is '^]'.
```

Note: Removed telnet to service.brightcloud.com over 443 since it never connects by design.

The device attempts to connect to BcapServer (service.brightcloud.com) on BcapPort (80) and DbServer (database.brightcloud.com) on SslPort (443).

If these connection attempts fails, the URL database is not downloaded .

Step 3. File Download Check

After confirming the domain connectivity with the required ports , you have to verify that the following files

have been finsihed downloading to the appliance.

```
root@123:#ls /var/sf/cloud_download/
```

```
root@123:#lsof | grep bcdb

SFDataCor 2516 root mem REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
SFDataCor 2516 root mem REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
SFDataCor 2516 root mem REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
SFDataCor 2516 root 54u REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
SFDataCor 2516 root 55u REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
SFDataCor 2516 root 61u REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2541 sfsnort mem REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2541 sfsnort mem REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2541 sfsnort mem REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2541 sfsnort 15u REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2541 sfsnort 16u REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2541 sfsnort 25u REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2542 sfsnort mem REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2542 sfsnort mem REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2542 sfsnort mem REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2542 sfsnort 15u REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2542 sfsnort 16u REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2542 sfsnort 25u REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2543 sfsnort mem REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2543 sfsnort mem REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2543 sfsnort mem REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2543 sfsnort 16u REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2543 sfsnort 25u REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2543 sfsnort 29u REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2549 sfsnort mem REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2549 sfsnort mem REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2549 sfsnort mem REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx
snort 2549 sfsnort 16u REG 0,11 480000000 573211 /dev/shm/Global.bcdb1
snort 2549 sfsnort 25u REG 0,11 129531946 573212 /dev/shm/Global.bcdb1acc
snort 2549 sfsnort 29u REG 0,11 262144 573213 /dev/shm/Global.bcdb1cacheinx

root@123:#pidof snort
2549 2543 2542 2541
```

When the local installation of URL dataset is complete, the file named full_bcdb_rep_4.xxx.bin is present in the/var/sf/cloud_download directory.

<#root>

```
root@123:# ls /var/sf/cloud_download/full_bcdb_rep_4.*
```

```
-rw-r--r--  1 root root 429M Mar 14 03:07 full_bcdb_rep_4.494.bin
```

Step 4. Restart SFDC

If some of the files are not downloaded completely or if they are missing from this folder location, you need to restart the following services to get the complete file download.

```
root@123:# pmtool restartbyid SFDataCorrelator
```

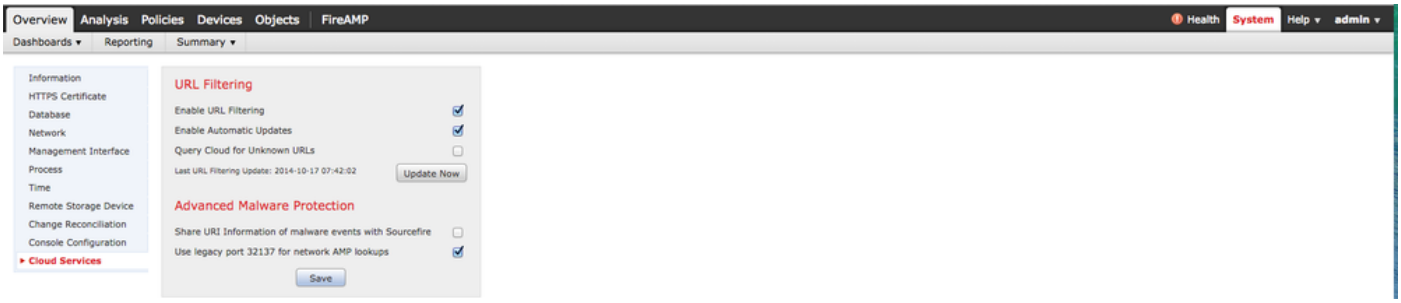
Step 5. Restart Snort Instance

```
root@123:# pmtool restartbytype snort
```

Step 6. Restart CloudAgent Service

```
root@123:# pmtool restartbyid CloudAgent
```

After restarting the required services , you need to attempt the URL update again from the Firesight Management Center.



Also verify the urldb_log file to verify the outputs. When CloudAgent is uptodate , then you can see the following output .

<#root>

```
root@123:# cd /var/log/
```

```
root@123:# tail -900f urldb_log

Jun 2 05:40:51 gw-iaps-01 SF-IMS[3769]: [3808] CloudAgent:CloudAgent [INFO] Nothing to do, up to date
Jun 2 05:40:53 gw-iaps-01 SF-IMS[3769]: [3808] CloudAgent:CloudAgent [INFO] Nothing to do, up to date
```

```
Jun 2 05:41:00 gw-iaps-01 SF-IMS[3769]: [3808] CloudAgent:CloudAgent [INFO] Nothing to do, up to date
Jun 2 05:41:01 gw-iaps-01 SF-IMS[3769]: [3808] CloudAgent:CloudAgent [INFO] Nothing to do, up to date
Jun 2 05:45:07 gw-iaps-01 SF-IMS[3769]: [3808] CloudAgent:CloudAgent [INFO] Nothing to do, up to date
```

Step 7. Perform Packet Capture

In some scenarios, even if the CloudAgent log file looks up-to-date, the telnet for the following is failed for 443/HTTPS connections:

```
root@123:# telnet service.brightcloud.com 443

Trying 54.221.218.187...

telnet: connect to address 54.221.218.187: Connection refused

Trying 107.22.214.128...

telnet: connect to address 107.22.214.128: Connection refused
```

If you notice such results, perform a packet capture using these steps.

1. SSH to the Firesight Management Center and elevate as root user with:

```
sudo su -
```

2. Run following command to start the capture.

```
tcpdump -i <interface> -s 0 -w /var/tmp/<file name>  port 443
```

To acquire the captures specifically to the cloud services , run the command in the following pattern . Make sure to give the option **–s** , otherwise the default size of packet is 96 bytes due to which the packets get truncated.

```
tcpdump -i <interface> -w testpcap1.pcap -s 9000 "host service.brightcloud.com or host database.brightc
```

3. If the issue is more frequent, then let the capture run till you see the failure health alert reappear. It would be good if you perform a telnet to both ports during the capture . (service.brightcloud and database.brightcloud).

4. Stop capture and **scp** the file to the server.

5. From the collected capture , confirm if the packets for 443 is triggering or if its getting dropped.

Step 8. Open a New Terminal and Run Debug

If the packets are not getting dropped and if you find that the packets are triggering successfully then it is quite possible that the CloudAgent has downloaded the URL Database but is failing the lookup for some specific unknown URLs.

While the capture is running you have to open a new terminal and run a debug for the CloudAgent. You would need to disable the CloudAgent process to do that.

Perform the following steps to start the debugs on the Firesight Management Center

Put cloud agent into debug mode by disabling the CloudAgent service.

```
root@123:# pmtool disablebyid CloudAgent
```

Run the Debug command for the CloudAgent

```
root@123:# CloudAgent --debug --config /etc/sf/cloudagent.conf --peers-config /etc/sf/device_cap.conf -
```

Once you are able to capture enough data , then stop the debug by terminating the CloudAgent process with the following command and thereafter re-enabling the CloudAgent service.

```
root@123:# pkill -15 CloudAgent
```

```
root@123:# pmtool enablebyid CloudAgent
```

The debug output looks like this:

```
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Setting debug level to
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Processing configurati
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Processing peer list c
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Processing cloud confi
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set cloud poll time to
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set queue memcap to 50
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set persistent cache m
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set request cache memc
```

```
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set ip reputation max
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set ip reputation max
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set ip reputation conn
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set ip reputation max
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] Set ip reputation auto
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] config file = /etc/sf/
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [INFO] pid file = /var/sf/run
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:158:ProcessC
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:250:auth_license_in
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:256:readSigFile(): File
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:263:auth_license_in
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:250:auth_license_in
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:277:readSigFile(): old_
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:543:verifyBuffer(): The
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:544:verifyBuffer(): The
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:629:rsa_verify(): Check
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:638:rsa_verify(): Possi
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:562:verifyBuffer(): Fou
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] key.c:595:verifyBuffer(): Val
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:291:auth_license_in
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1103:load_kvp(): Ca
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1121:load_kvp(): kv
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1121:load_kvp(): kv
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1121:load_kvp(): kv
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1121:load_kvp(): kv
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1121:load_kvp(): kv
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:421:auth_license_va
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1345:auth_search_fo
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:447:auth_license_va
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:463:auth_license_va
Jul 20 05:36:23 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:250:auth_license_in

Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:421:auth_license_va
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:1345:auth_search_fo
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:437:auth_license_va
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:447:auth_license_va
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:463:auth_license_va
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:AUTH [DEBUG] license.c:564:auth_license_va
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:405:GetURLFi
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:479:Get
URLFilteringLicenseInfo(): count for model 72H(URLFilter) is 2
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:171:ProcessC
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:DM_peers [DEBUG] DM_peers.c:111:add_peer()
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:DM_peers [DEBUG] DM_peers.c:118:add_peer()
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:344:ProcessU
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:DM_peers [DEBUG] DM_peers.c:151:PrintPeers
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:346:ProcessU
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:DM_peers [DEBUG] DM_peers.c:111:add_peer()
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:DM_peers [DEBUG] DM_peers.c:118:add_peer()
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:344:ProcessU
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:DM_peers [DEBUG] DM_peers.c:151:PrintPeers
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:DM_peers [DEBUG] DM_peers.c:151:PrintPeers
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:346:ProcessU
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:350:ProcessU
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:cloud_config [DEBUG] config.c:178:ProcessC
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:SFTL [DEBUG] SSLSupport.c:26:init_OpenSSL(
Jul 20 05:36:24 bne-fsm-01 SF-IMS[27417]: [27417] CloudAgent:CloudAgent [DEBUG] CloudAgent.cpp:278:main
```

Step 9. Perform Tests

If the debug looks fine as well as the url db logs also state that nothing to update, you have to perform one more test to confirm if the triggered cloud lookup alert is a false positive or not .

To perform the following test, you must arrange a maintenance window .

Test -1

Perform the backup for bcdb files from the FireSIGHT Management Center and Firepower.

The files for which you need to perform the backup is available in the following location.

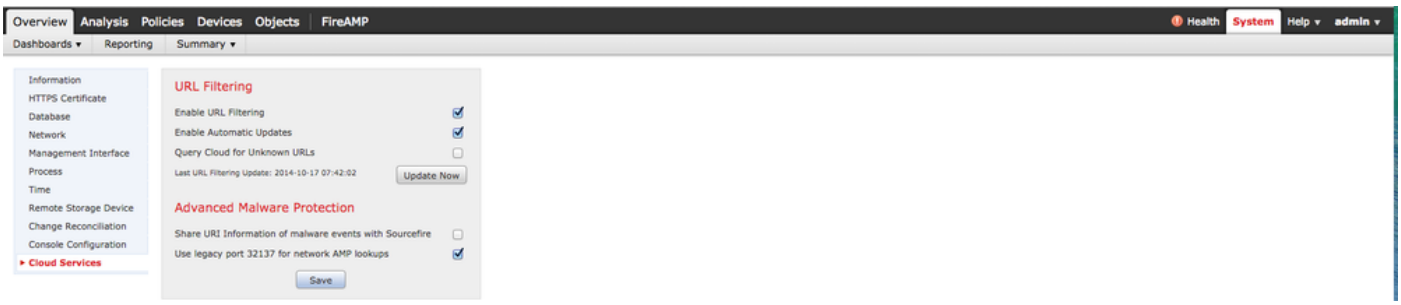
```
root@123:# cd /var/sf/cloud_download/
```

Move the files from this location to a different location in the FireSIGHT Management Center and Firepower.

Once you take back up, remove the bcdb files from /var/sf/cloud_download/ locations and perform a force download of database by performing the next steps.

Log in to the FireSIGHT Management Center and navigate to **System > Local > Configuration > Cloud Services**.

Click on the **Update Now** button.



Check if the new bcdb files are getting updated successfully in same location /var/sf/cloud_download/ in the FireSIGHT Management Center. If it is freshly downloading in the FireSIGHT Management Center, you need to push the access control policy to ensure that the same database files are updated in the Firepower (managed sensor).

If you could not download the files successfully, recopy the bcdb files to same location inside /var/sf/cloud_download/ so that it does not affect anything.

Test -2

Perform the **url lookup** (perform the url lookup for a url which is not present/available in the database) and reconfirm the response.

If the files reappear after the test was performed once the database files were deleted from the /var/sf/cloud_downloads, it means that the connections on 443 were successful.

Conclusion

Sometime the cloud lookup errors are intermittent. In versions such as 5.3.1.2, there is a possibility that health monitoring module reports false positive alerts for the cloud lookup errors.The intermittent health lookup alert provides a report that looks like this:

```
Health Monitor Alert from abc.com
Time: youd Aug  5 12:01:41 2015 UTC
Severity: critical
Module: URL Filtering Monitor
Description: Cloud lookup failure

Health Monitor Alert from abc.com
Time: youd Aug  5 12:17:03 2015 UTC
Severity: recovery
Module: URL Filtering Monitor
Description: Process is running correctly
```

After confirming that all the tests were successful and if you still receive the intermittent cloud lookup errors, this is an issue with the health alarm being too sensitive as of version 5.3.1.2. The Cisco bug CSCut77594 has been reported to this respect. The health alarm triggers even when there is one failure for a **url lookup**, and failure means that you did not get a response from the brightcloud server for that particular URL. False positive issues with the URL health monitoring module have been fixed in these versions:

DRAMBUIE 5.4.1.5_KENTON 5.4.0.6_AND_5.4.1.5_DC 5.3.1.7 5.3.0.8