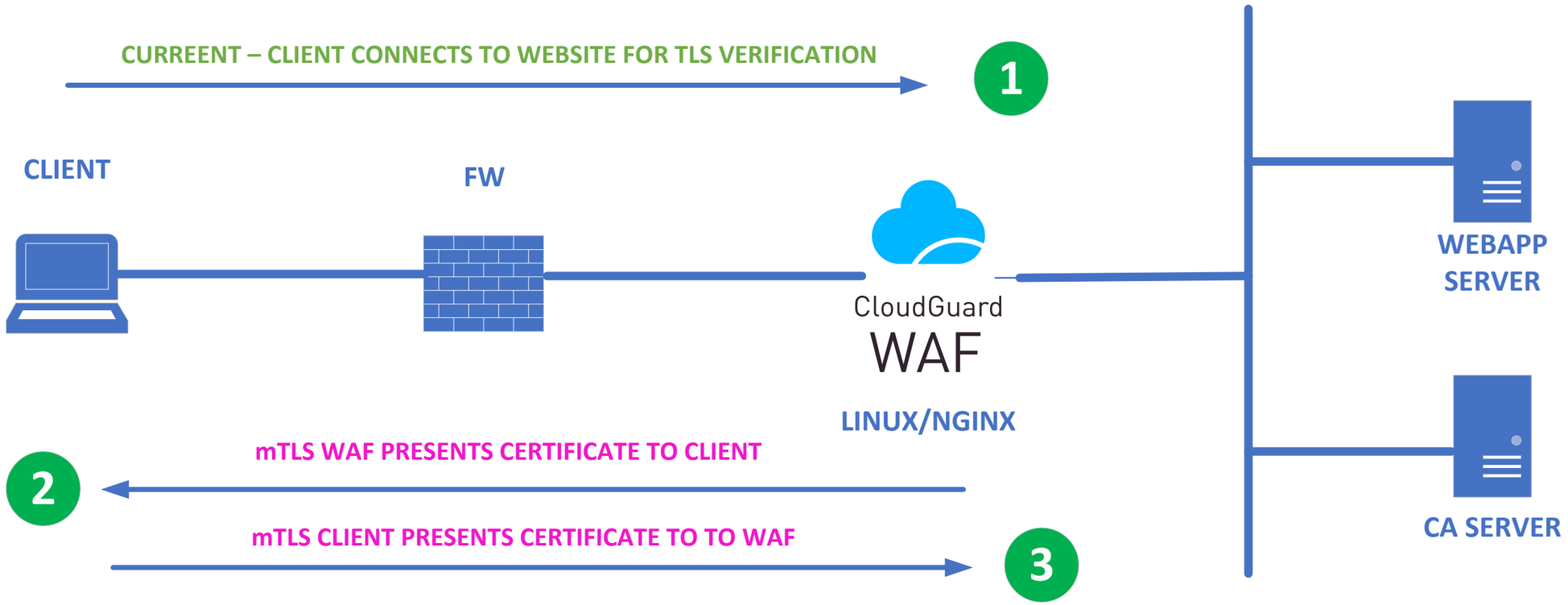
Mutual TLS



This is an extension/additional layer of TLS verification of the current TLS client to WAF verification where the **WAF will now challenge** the client to present the rootCA(Client cert) to the WAF to complete the mTLS process.

CG WAF OVA Agent - mTLS
mTLS Steps:

Requirements - Obtain rootCA.crt

Phase#1

Copying the rootCA.crt to the docker container.

1. SSH to the OVA Instance
2. docker ps -a # To see all containers such as cp_nginx_gaia
3. docker exec -it cp_nginx_gaia sh #access the docker containers with shell
4. cd /etc/nginx/conf.d
5. ls -ll #To view your domain name conf file

example: 443_example.com.conf

6. cat 443_example.com.conf #to view the path of where the ssl cert directory is located.

example: ssl_certificate /etc/cp/rpmanager/manualCerts/

7. Using WINSCP, SCP to the OVA agent and copy the rootCA.crt to the path in step 6, /etc/cp/rpmanager/manualCerts/

Phase#2

Adding the location file and server block to the Check Point UI

1. Create 2 txt files for the location and server block. Pay attention to any spaces at the end of the last character and delete them.

Save file as locationblock.txt

```
if ($ssl_client_verify != SUCCESS) {
    return 403;
}
```

Save file as serverblock.txt # Pay attention to any spaces at the end of the last character and delete them.

```
ssl_client_certificate /etc/cp/rpmanager/manualCerts/rootCA.crt;
ssl_verify_client      on; # or optional
```

1. Logon to the CHKP Portal>CloudGuard>WAF>Assets>Your domain asset
2. Under the General tab, click on Advanced below the Reverse Proxy Section
3. Click on Additional Settings
4. Add a checkmark for Additional location block and upload the your locationblock.txt file.
5. Add a checkmark for Additional server block and upload the your serverblock.txt file.
6. Enforce

You should not see any critical events in the Asset event section if done properly.

Phase3#

Verify that the location and server files were added to /etc/nginx/conf.d/443_example.com.conf

1. Connect to the docker container as you did in Phase#1, step3
2. cat /etc/nginx/conf.d/443_example.com.conf #to view that the file includes the location and server block sections

Example: You will see this for the location in the file

```
include   /etc/cp/conf/rpmanager/include/example_-_mTLS_additional_location_config.conf;
```

You will see this for the server in the file

```
include /etc/cp/conf/rpmanager/include/example_-_mTLS_additional_server_config.conf;
```

3. To actually see that the settings for the 2 files in Phase2#, step1 were added, do the following:

cat /etc/cp/conf/rpmanager/include/example_-_mTLS_additional_server_config.conf

Output:
```
ssl_client_certificate /etc/cp/rpmanager/manualCerts/rootCA.crt;
    ssl_verify_client      on;
```

cat /etc/cp/conf/rpmanager/include/example_-_mTLS_additional_location_config.conf

Output:
```
if ($ssl_client_verify != SUCCESS) {
        return 403;
    }
```