

Test Plan for SecureGate Proxy

Step 1: Setup the Test Environment

1. Ensure Python 3, net-tools, and tcpdump are installed.

2. Install required tools using:

```
sudo apt update && sudo apt install python3 net-tools tcpdump -y
```

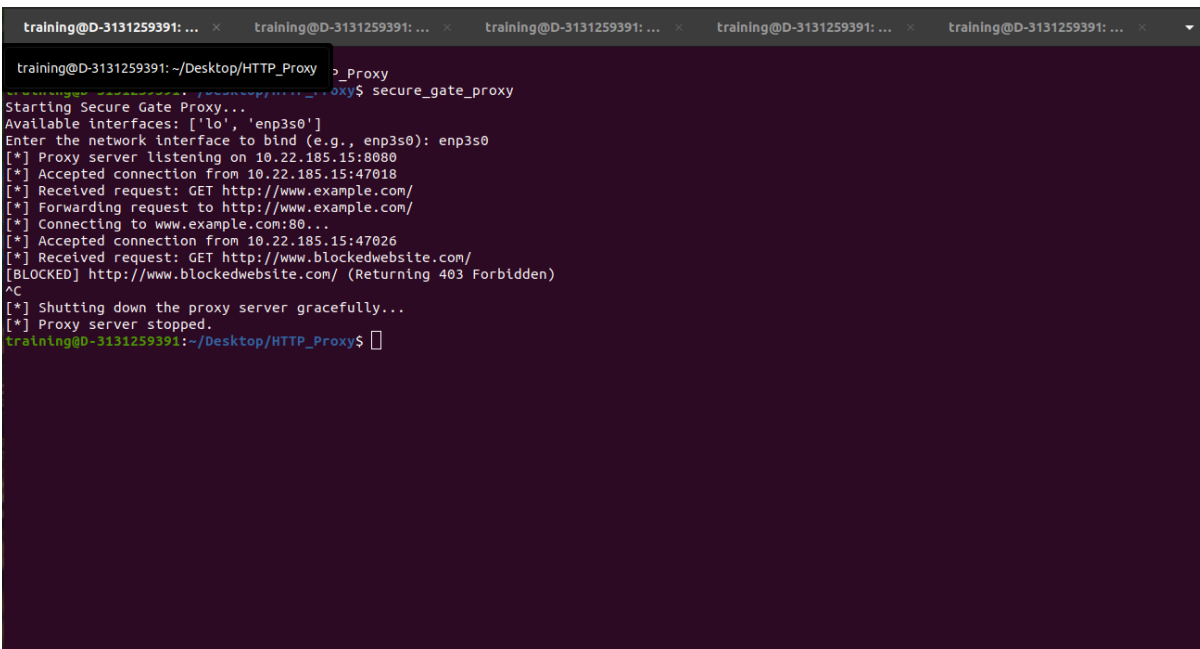
Step 2: Start the Proxy Server

Run the command:

```
python3 http_proxy.py
```

Expected Output:

```
[*] Proxy server listening on <Your-Management-IP>:8080
```

A screenshot of a terminal window with a dark purple background. The terminal shows the execution of the 'secure_gate_proxy' command. The output includes: 'Starting Secure Gate Proxy...', 'Available interfaces: ['lo', 'enp3s0']', 'Enter the network interface to bind (e.g., enp3s0): enp3s0', '[*] Proxy server listening on 10.22.185.15:8080', '[*] Accepted connection from 10.22.185.15:47018', '[*] Received request: GET http://www.example.com/', '[*] Forwarding request to http://www.example.com/', '[*] Connecting to www.example.com:80...', '[*] Accepted connection from 10.22.185.15:47026', '[*] Received request: GET http://www.blockedwebsite.com/', '[BLOCKED] http://www.blockedwebsite.com/ (Returning 403 Forbidden)', '^C', '[*] Shutting down the proxy server gracefully...', and '[*] Proxy server stopped.' The prompt 'training@D-3131259391:~/Desktop/HTTP_Proxy\$' is visible at the bottom.

```
training@D-3131259391: ~/Desktop/HTTP_Proxy$ secure_gate_proxy
Starting Secure Gate Proxy...
Available interfaces: ['lo', 'enp3s0']
Enter the network interface to bind (e.g., enp3s0): enp3s0
[*] Proxy server listening on 10.22.185.15:8080
[*] Accepted connection from 10.22.185.15:47018
[*] Received request: GET http://www.example.com/
[*] Forwarding request to http://www.example.com/
[*] Connecting to www.example.com:80...
[*] Accepted connection from 10.22.185.15:47026
[*] Received request: GET http://www.blockedwebsite.com/
[BLOCKED] http://www.blockedwebsite.com/ (Returning 403 Forbidden)
^C
[*] Shutting down the proxy server gracefully...
[*] Proxy server stopped.
training@D-3131259391:~/Desktop/HTTP_Proxy$
```

Step 3: Verify Proxy is Running

Check if proxy is listening:

```
netstat -tulnp | grep 8080
```

Expected Output:

```
tcp <Your-Management-IP>:8080 LISTEN <Process ID>
```

```
training@D-31312... x training@D-31312... x training@D-31312... x training@D-31312... x training@D-31312... x training@D-31312... x
training@D-3131259391:~/Desktop/HTTP_Proxy$ netstat -tulnp | grep 8080
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:8080          0.0.0.0:*           LISTEN      226743/python3
training@D-3131259391:~/Desktop/HTTP_Proxy$
```

Step 4: Direct Request Without Proxy

Test direct request:

```
curl -vvv http://www.example.com -o /dev/null
```

Expected Output:

HTTP/1.1 200 OK

```
training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x
training@D-3131259391:~/Desktop/HTTP_Proxy$ curl -vvv http://www.example.com -o /dev/null
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left   Speed
  0     0    0     0    0     0      0      0  0 --:--:-- --:--:-- --:--:--    0*   Trying 173.223.235.10:80...
* TCP_NODELAY set
* Connected to www.example.com (173.223.235.10) port 80 (#0)
> GET / HTTP/1.1
> Host: www.example.com
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Content-Type: text/html
< ETag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"
< Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT
< Cache-Control: max-age=2967
< Date: Thu, 27 Mar 2025 04:10:06 GMT
< Content-Length: 1256
< Connection: keep-alive
<
{ [1256 bytes data]
100 1256 100 1256    0     0 16746    0 --:--:-- --:--:-- --:--:-- 16972
* Connection #0 to host www.example.com left intact
training@D-3131259391:~/Desktop/HTTP_Proxy$
```

Step 5: Send HTTP Requests via Proxy

Test an allowed URL:

VIA: 1.1 secure_gate_proxy

HTTP/1.1 403 Forbidden

```

training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x
training@D-3131259391:~/Desktop/HTTP_Proxy$ curl -vvv -x 10.22.185.15:8080 http://www.blockedwebsite.com -o/dev/null
* Trying 10.22.185.15:8080...
* TCP_NODELAY set
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
0      0    0     0    0  0 --:--:-- --:--:-- --:--:--    0* Connected to 10.22.185.15 (10.22.185.15) port 8080 (#0)
> GET http://www.blockedwebsite.com/ HTTP/1.1
> Host: www.blockedwebsite.com
> User-Agent: curl/7.68.0
> Accept: */*
> Proxy-Connection: Keep-Alive
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 403 Forbidden
< Content-Length: 18
<
[ 14 bytes data]
* transfer closed with 4 bytes remaining to read
77    18   77   14    0  4666    0 --:--:-- --:--:-- --:--:--  4666
* Closing connection 0
curl: (18) transfer closed with 4 bytes remaining to read
training@D-3131259391:~/Desktop/HTTP_Proxy$

```

Step 7: Capture Proxy Traffic Using tcpdump

Start packet capture:

```
sudo tcpdump -i enp3s0 port 8080 -n
```

Expected Output:

Shows packet logs when requests are made.

```
training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x
0x05c0: 3c70 3e3c 6120 6872 6566 3d22 6874 7470 <p><a.href="http
0x05d0: 733a 2f2f 7777 772e 6961 6e61 2e6f 7267 s://www.iana.org
0x05e0: 2f64 6f6d 6169 6e73 2f65 7861 6d70 6c65 /domains/example
0x05f0: 223e 4d6f 7265 2069 6e66 6f72 6d61 7469 ">More.informati
0x0600: 6f6e 2e2e 2e3c 2f61 3e3c 2f70 3e0a 3c2f on...</a></p></
0x0610: 6469 763e 0a3c 2f62 6f64 793e 0a3c 2f68 div></body></h
0x0620: 746d 6c3e 0a tml>
09:40:48.784283 IP 173.223.235.10.80 > 10.22.185.15.60728: Flags [F.], seq 1522, ack 132, win 509, options [nop,nop,TS val 1955619285 ecr 3741
033838], length 0
0x0000: 4520 0034 6586 4000 3706 820e addf eb0a E..4e.@.7.....
0x0010: 0a16 b90f 0050 ed38 4205 e0b7 c259 e52d ....P.8B....Y.-
0x0020: 8011 01fd 0612 0000 0101 080a 7490 61d5 .....t.a.
0x0030: defb a56e ...n
09:40:48.784289 IP 10.22.185.15.60728 > 173.223.235.10.80: Flags [.], ack 1522, win 499, options [nop,nop,TS val 3741033840 ecr 1955619285], l
length 0
0x0000: 4500 0034 4cf3 4000 4006 91c1 0a16 b90f E..4L.@.7.....
0x0010: addf eb0a ed38 0050 c259 e52d 4205 e0b7 ....8.P.Y.-B...
0x0020: 8010 01f3 5c36 0000 0101 080a defb a570 ....\6.....p
0x0030: 7490 61d5 t.a.
09:40:48.784420 IP 10.22.185.15.60728 > 173.223.235.10.80: Flags [F.], seq 132, ack 1523, win 501, options [nop,nop,TS val 3741033840 ecr 1955
619285], length 0
0x0000: 4500 0034 4cf4 4000 4006 91c0 0a16 b90f E..4L.@.7.....
0x0010: addf eb0a ed38 0050 c259 e52d 4205 e0b8 ....8.P.Y.-B...
0x0020: 8011 01f5 5c36 0000 0101 080a defb a570 ....\6.....p
0x0030: 7490 61d5 t.a.
09:40:48.785118 IP 173.223.235.10.80 > 10.22.185.15.60728: Flags [.], ack 133, win 509, options [nop,nop,TS val 1955619286 ecr 3741033840], le
ngth 0
0x0000: 4520 0034 6587 4000 3706 820d addf eb0a E..4e.@.7.....
0x0010: 0a16 b90f 0050 ed38 4205 e0b8 c259 e52e ....P.8B....Y..
0x0020: 8010 01fd 060e 0000 0101 080a 7490 61d6 .....t.a.
0x0030: defb a570 ...p
^C
20 packets captured
20 packets received by filter
0 packets dropped by kernel
training@D-3131259391:~/Desktop/HTTP_Proxy$
```

Step 8: Stop the Proxy and Cleanup

Stop the proxy:

Press CTRL+C in the terminal running http_proxy.py

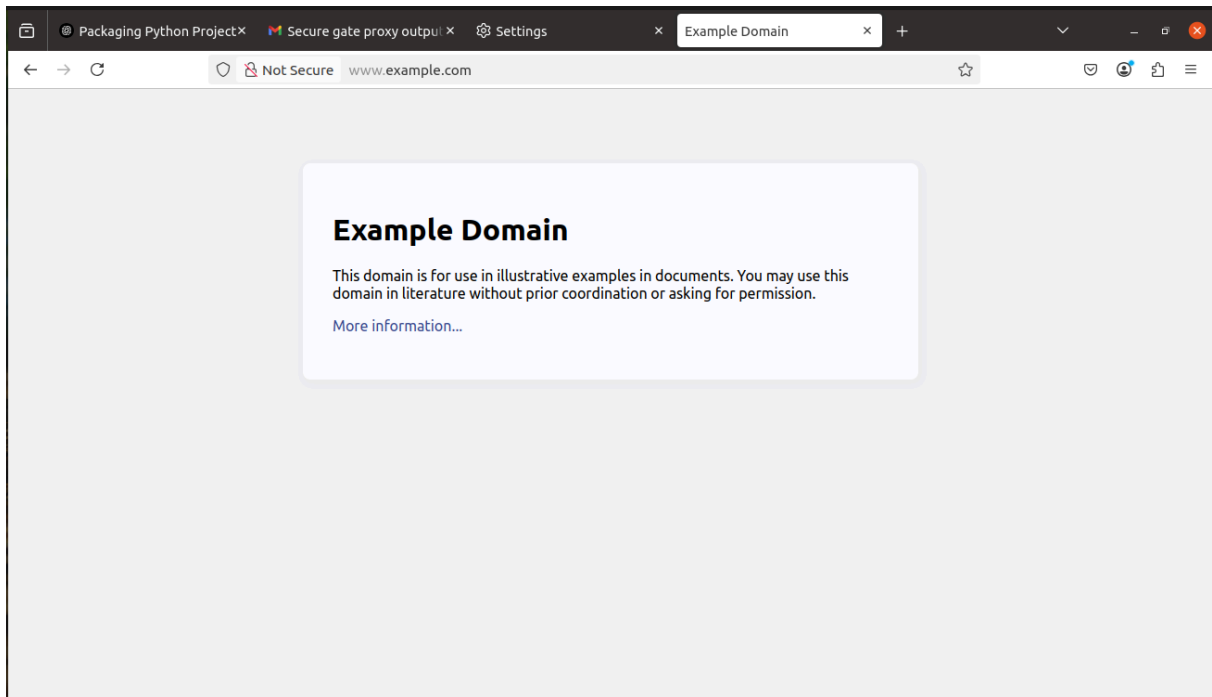
Expected Output:

[*] Shutting down the proxy server.

```
training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ... x training@D-3131259391: ...
training@D-3131259391: ~/Desktop/HTTP_Proxy$ sudo secure_gate_proxy
Starting Secure Gate Proxy...
Available interfaces: ['lo', 'enp3s0']
Enter the network interface to bind (e.g., enp3s0): enp3s0
[*] Proxy server listening on 10.22.185.15:8080
[*] Accepted connection from 10.22.185.15:47018
[*] Received request: GET http://www.example.com/
[*] Forwarding request to http://www.example.com/
[*] Connecting to www.example.com:80...
[*] Accepted connection from 10.22.185.15:47026
[*] Received request: GET http://www.blockedwebsite.com/
[BLOCKED] http://www.blockedwebsite.com/ (Returning 403 Forbidden)
^C
[*] Shutting down the proxy server gracefully...
[*] Proxy server stopped.
training@D-3131259391:~/Desktop/HTTP_Proxy$
```

BROWSER TESTS:

ALLOWED URL:



BLOCKED URL:

