Skyhigh Security

# SWG troubleshooting and common scenarios

May 2023

Skyhigh Security

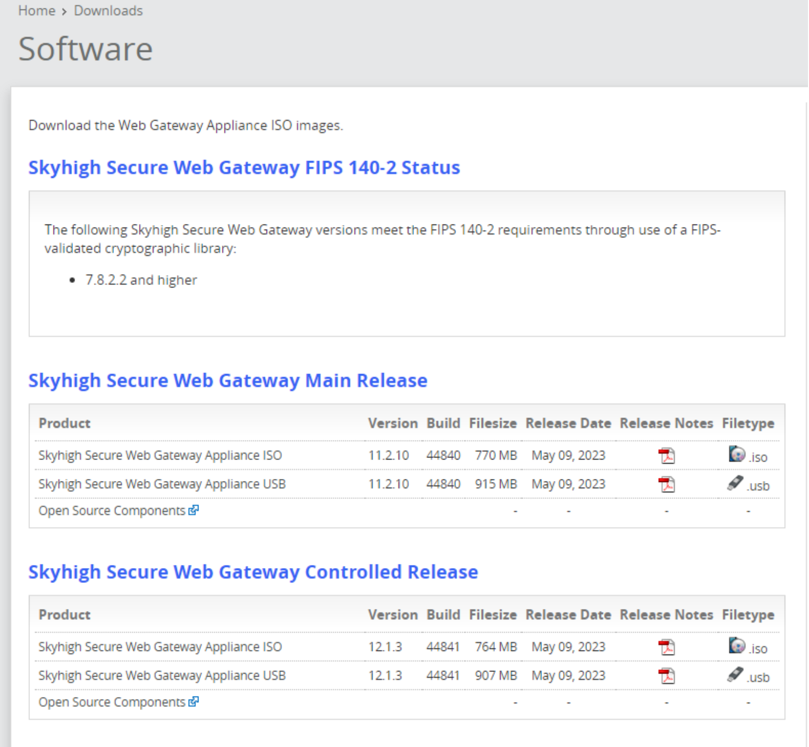
## Overview

- Software/License
- How to submit a hardware issue
- SWG Troubleshooting
- Perfect Case/SR

# Software & License

- SWG Software & License
  [https://contentsecurity.skyhigh.cloud](https://contentsecurity.skyhigh.cloud)
- Skyhigh Client Proxy (SCP), CSR & others
  [https://success.myshn.net/Software_Downloads](https://success.myshn.net/Software_Downloads)

  [https://www.trellix.com/en-us/downloads.html](https://www.trellix.com/en-us/downloads.html)
- License issues SWG:
  Contact licensing@trellix.com
- SWG documentation:
  [https://success.myshn.net/Skyhigh_Secure_Web_Gateway_(On_Prem)](https://success.myshn.net/Skyhigh_Secure_Web_Gateway_(On_Prem))



Home › Downloads

## Software

Download the Web Gateway Appliance ISO images.

### Skyhigh Secure Web Gateway FIPS 140-2 Status

The following Skyhigh Secure Web Gateway versions meet the FIPS 140-2 requirements through use of a FIPS-validated cryptographic library:

- 7.8.2.2 and higher

### Skyhigh Secure Web Gateway Main Release

| Product | Version | Build | Filesize | Release Date | Release Notes | Filetype |
|---|---|---|---|---|---|---|
| Skyhigh Secure Web Gateway Appliance ISO | 11.2.10 | 44840 | 770 MB | May 09, 2023 |  | .iso |
| Skyhigh Secure Web Gateway Appliance USB | 11.2.10 | 44840 | 915 MB | May 09, 2023 |  | .usb |
| Open Source Components |  |  | - | - | - | - |

### Skyhigh Secure Web Gateway Controlled Release

| Product | Version | Build | Filesize | Release Date | Release Notes | Filetype |
|---|---|---|---|---|---|---|
| Skyhigh Secure Web Gateway Appliance ISO | 12.1.3 | 44841 | 764 MB | May 09, 2023 |  | .iso |
| Skyhigh Secure Web Gateway Appliance USB | 12.1.3 | 44841 | 907 MB | May 09, 2023 |  | .usb |
| Open Source Components |  |  | - | - | - | - |

# Hardware Troubleshooting

- How to submit a hardware issue to the Web Gateway Technical Support team

  https://kcm.trellix.com/corporate/index?page=content&id=KB89685

Required data:

- Getlogs script (hardware log) – Details on how to install and run can also be found on:

  https://success.myshn.net/Skyhigh_Secure_Web_Gateway_(On_Prem)/Best_Practices/Hardware_and_Applicance_Maintenance/Collect_Hardware_Logs_(getlogs)
- Information from KB (serial, contact- and shipping information)

- For all hardware topics such as:
- RAID reports 1 critical disks and 1 failing disks
- BBU - Battery replacement required
- Failure of the power supply unit

# Secure Web Gateway Troubleshooting

- Feedback file
- Rule traces (identify delays, flow through policy)
- GTI delays
- Tcpdump / Network Tools (packet flow, network communication)
- Connection traces (what is proxy engine doing, needed for SSL/HSM/FTP and more)
- Core file (memory dump, identify resource usage issue)
- Auth. debug (identify auth. issues)
- Common issues

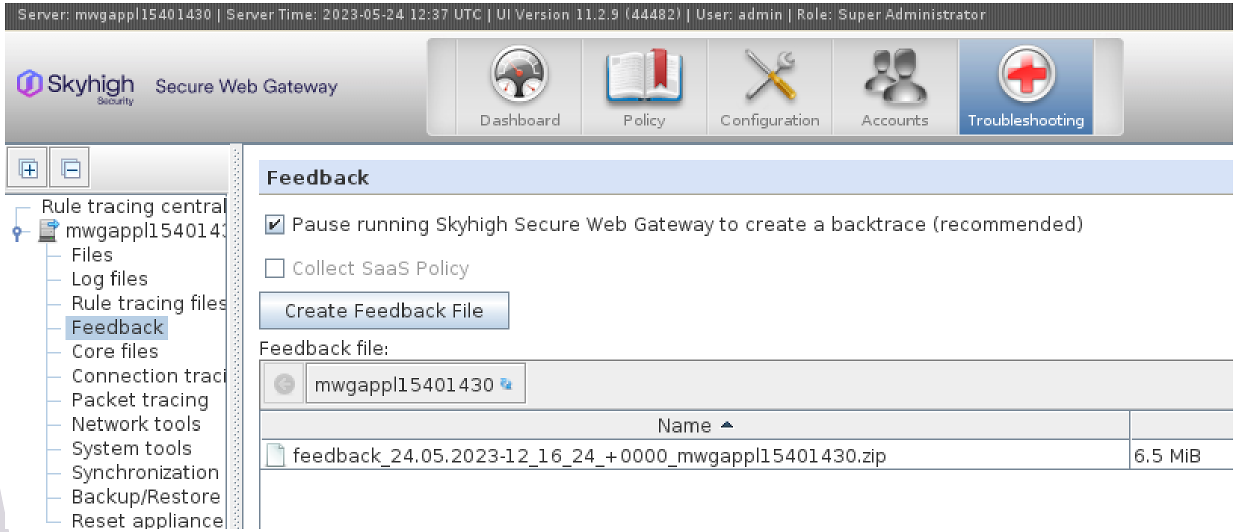
# Secure Web Gateway Troubleshooting - Feedback File

Troubleshooting > Feedback

[https://success.myshn.net/Skyhigh_Secure_Web_Gateway_(On_Prem)/Troubleshooting/Create_a_Feedback_File](https://success.myshn.net/Skyhigh_Secure_Web_Gateway_(On_Prem)/Troubleshooting/Create_a_Feedback_File)

CLI:

-
  ```
  cd /opt/mwg/bin
  ./feedback.sh
  ```
- Choose level 2
- After the script has finished, you will find the feedback file in */opt/mwg/log/debug/feedbacks*.



Server: mwgappl15401430 | Server Time: 2023-05-24 12:37 UTC | UI Version 11.2.9 (44482) | User: admin | Role: Super Administrator

**Feedback**

☑ Pause running Skyhigh Secure Web Gateway to create a backtrace (recommended)

☐ Collect SaaS Policy

Create Feedback File

Feedback file:

mwgappl15401430

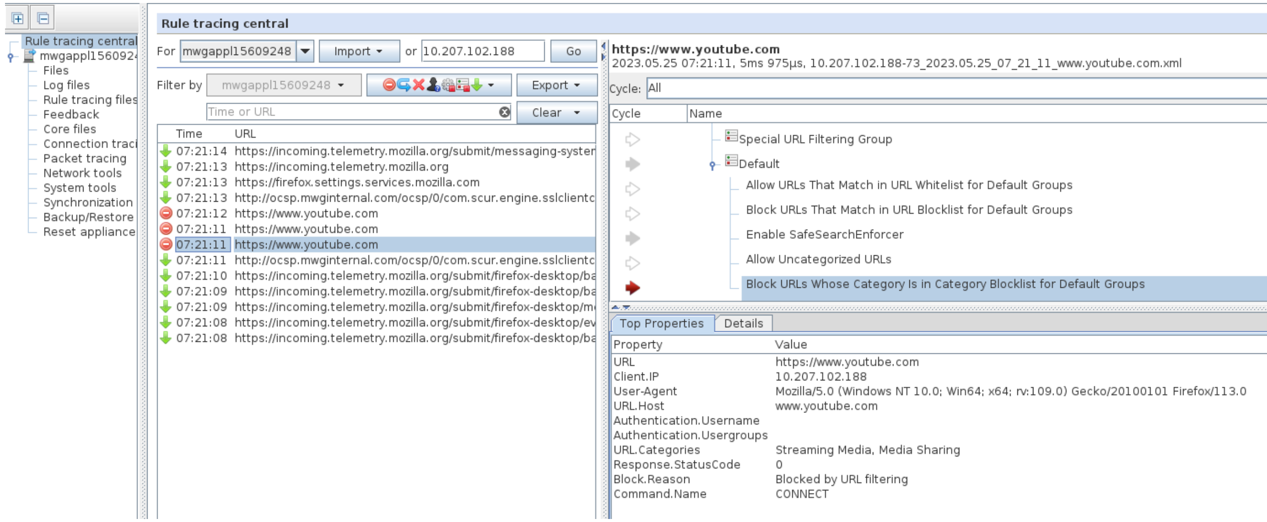
| Name ▲ | |
|---|---|
| feedback_24.05.2023-12_16_24_+0000_mwgappl15401430.zip | 6.5 MiB |

# Secure Web Gateway Troubleshooting - Rule Traces

- Troubleshooting > Rule Tracing Central

Tracing information is displayed for the following:

  - **Cycles**
  - **Rules**
  - **Rule sets**
  - **Rule Criteria**
  - **Properties**
  - **Events**



Rule tracing central

For mwgappl15609248 Import or 10.207.102.188 Go

Filter by mwgappl15609248

Time or URL

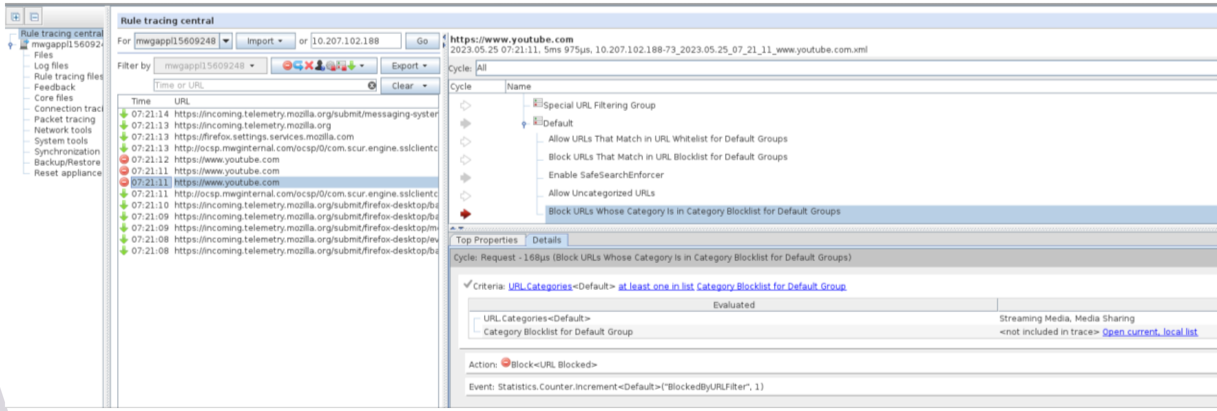
```
Time      URL
07:21:14  https://incoming.telemetry.mozilla.org/submit/messaging-syster
07:21:13  https://incoming.telemetry.mozilla.org
07:21:13  https://firefox.settings.services.mozilla.com
07:21:13  http://ocsp.mwginternal.com/ocsp/0/com.scur.engine.sslclientc
07:21:12  https://www.youtube.com
07:21:11  https://www.youtube.com
07:21:11  https://www.youtube.com
07:21:11  http://ocsp.mwginternal.com/ocsp/0/com.scur.engine.sslclientc
07:21:10  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ba
07:21:09  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ba
07:21:09  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/m
07:21:08  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ev
07:21:08  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ba
```

**https://www.youtube.com**
2023.05.25 07:21:11, 5ms 975μs, 10.207.102.188-73_2023.05.25_07_21_11_www.youtube.com.xml

Cycle: All

```
Cycle  Name
         Special URL Filtering Group
         Default
           Allow URLs That Match in URL Whitelist for Default Groups
           Block URLs That Match in URL Blocklist for Default Groups
           Enable SafeSearchEnforcer
           Allow Uncategorized URLs
           Block URLs Whose Category Is in Category Blocklist for Default Groups
```

| Property | Value |
|---|---|
| URL | https://www.youtube.com |
| Client.IP | 10.207.102.188 |
| User-Agent | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0 |
| URL.Host | www.youtube.com |
| Authentication.Username | |
| Authentication.Usergroups | |
| URL.Categories | Streaming Media, Media Sharing |
| Response.StatusCode | 0 |
| Block.Reason | Blocked by URL filtering |
| Command.Name | CONNECT |



Rule tracing central

For mwgappl15609248 Import or 10.207.102.188 Go

Filter by mwgappl15609248

Time or URL

```
Time      URL
07:21:14  https://incoming.telemetry.mozilla.org/submit/messaging-syster
07:21:13  https://incoming.telemetry.mozilla.org
07:21:13  https://firefox.settings.services.mozilla.com
07:21:13  http://ocsp.mwginternal.com/ocsp/0/com.scur.engine.sslclientc
07:21:12  https://www.youtube.com
07:21:11  https://www.youtube.com
07:21:11  https://www.youtube.com
07:21:11  http://ocsp.mwginternal.com/ocsp/0/com.scur.engine.sslclientc
07:21:10  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ba
07:21:09  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ba
07:21:09  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/m
07:21:08  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ev
07:21:08  https://incoming.telemetry.mozilla.org/submit/firefox-desktop/ba
```

**https://www.youtube.com**
2023.05.25 07:21:11, 5ms 975μs, 10.207.102.188-73_2023.05.25_07_21_11_www.youtube.com.xml

Cycle: All

```
Cycle  Name
         Special URL Filtering Group
         Default
           Allow URLs That Match in URL Whitelist for Default Groups
           Block URLs That Match in URL Blocklist for Default Groups
           Enable SafeSearchEnforcer
           Allow Uncategorized URLs
           Block URLs Whose Category Is in Category Blocklist for Default Groups
```

Cycle: Request - 168μs (Block URLs Whose Category Is in Category Blocklist for Default Groups)

✓ Criteria: URL.Categories<Default> at least one in list Category Blocklist for Default Group

| Evaluated | |
|---|---|
| URL.Categories<Default> | Streaming Media, Media Sharing |
| Category Blocklist for Default Group | <not included in trace> Open current, local list |

Action: Block<URL Blocked>

Event: Statistics.Counter.Increment<Default>("BlockedByURLFilter", 1)

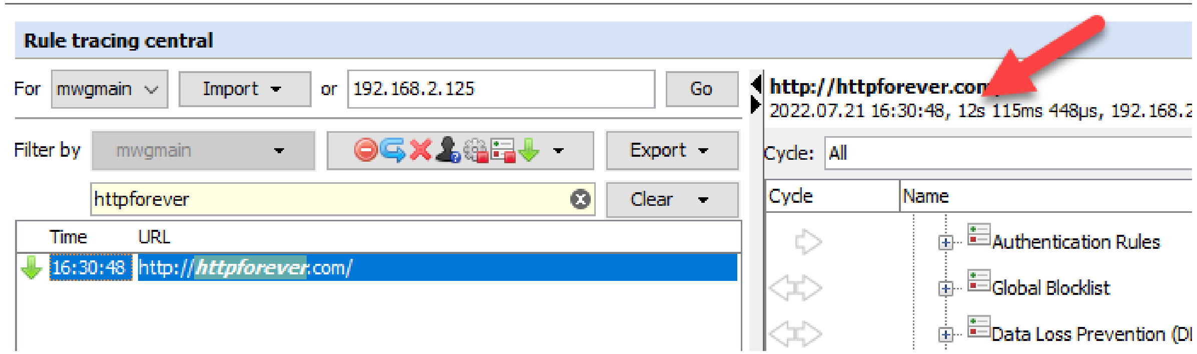
# Secure Web Gateway Troubleshooting - GTI delays

GTI is the Global Threat Intelligence service and a requirement for the web gateway to function correctly.

Failure to allow access to the GTI servers correctly will cause noticeable and direct delays (up to 12 seconds)

[https://kcm.trellix.com/corporate/index?page=content&id=KB90854](https://kcm.trellix.com/corporate/index?page=content&id=KB90854)

[https://kcm.trellix.com/corporate/index?page=content&id=KB79640](https://kcm.trellix.com/corporate/index?page=content&id=KB79640)



Rule tracing central

For: mwgmain  Import  or  192.168.2.125  Go

Filter by: mwgmain

httpforever

| Time | URL |
|---|---|
| 16:30:48 | http://httpforever.com/ |

http://httpforever.com

2022.07.21 16:30:48, 12s 115ms 448µs, 192.168.2

Cycle: All

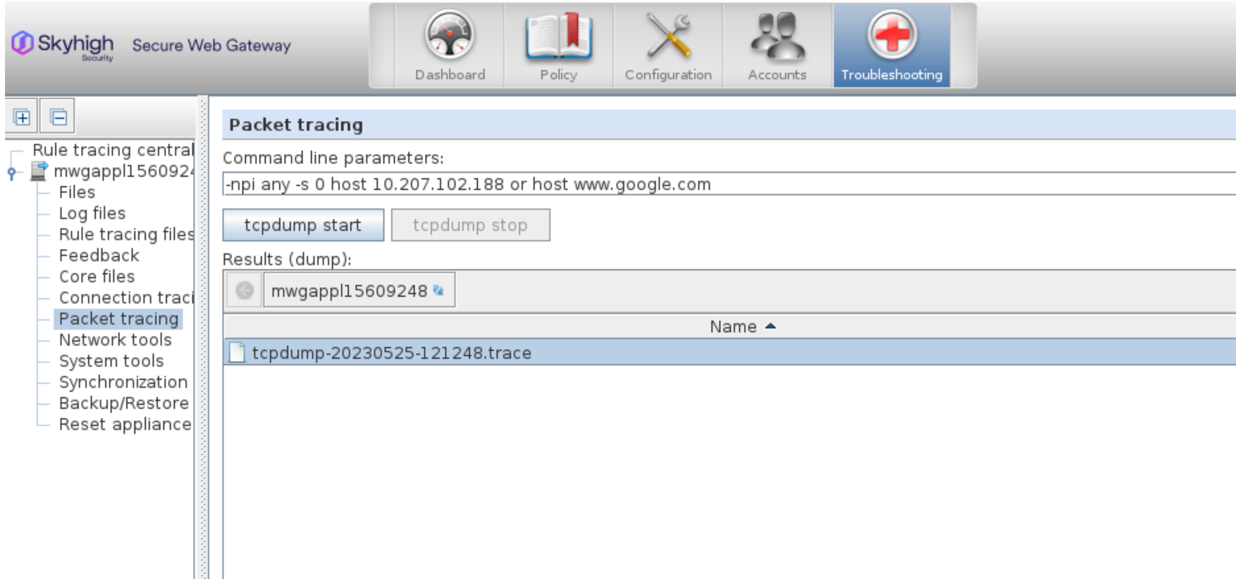
| Cycle | Name |
|---|---|
| | Authentication Rules |
| | Global Blocklist |
| | Data Loss Prevention (Dl |

# Secure Web Gateway Troubleshooting – TCP Dump & Network tools

Network tools, general troubleshooting initial checks for connectivity.

Packet Tracing also verbally known as TCPDump capturing packets on the network for in-depth investigation.

https://success.myshn.net/Skyhigh_Secure_Web_Gateway_(On_Prem)/Best_Practices/Write_a_Playbook/Performing_Packet_Tracing_in_Secure_Web_Gateway_(SWG)



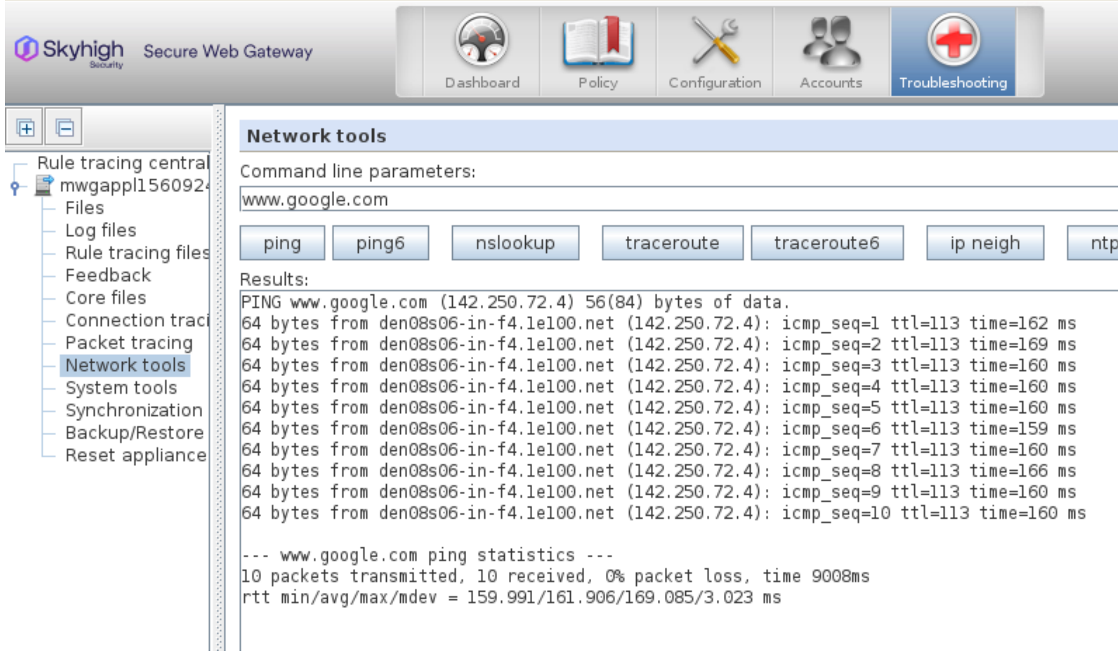
Packet tracing

Command line parameters:

```
-npi any -s 0 host 10.207.102.188 or host www.google.com
```

Results (dump): mwgappl15609248

tcpdump-20230525-121248.trace



Network tools

Command line parameters:

```
www.google.com
```

Results:

```
PING www.google.com (142.250.72.4) 56(84) bytes of data.
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=1 ttl=113 time=162 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=2 ttl=113 time=169 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=3 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=4 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=5 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=6 ttl=113 time=159 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=7 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=8 ttl=113 time=166 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=9 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=10 ttl=113 time=160 ms

--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008ms
rtt min/avg/max/mdev = 159.991/161.906/169.085/3.023 ms
```

# Secure Web Gateway Troubleshooting - Tcpdump & Network Tools - cont

Troubleshooting > Packet Tracing | Network Tools

Common parameters for packet tracing:

- -s (snap length - amount of data for each frame; 0 no limit)
- -i (Listen on defined interface / any = all interfaces)
- host (can be hostname or IP - www.skyhighsecurity.com or host 10.11.12.13)
- port (the port you want to capture)

Example for filter on NTLM authentication issues:

```
–s 0 –i any host <clientIP> or port 445 or port 53
```

Rolling tcpdump from SWG CLI:

```
nohup tcpdump -Z root -s 0 -i any host x.x.x.x or host x.x.x.x  -C 100 -W 20 -w capturefilename.pcap &
```

- -C is how large the capture can be before a new one is started in MB
- -W is how many files before the oldest is deleted
- & run in background

# Secure Web Gateway Troubleshooting - Tcpdump & Network Tools - cont

Running rolling tcpdump in background:

After putting in the command and you hit enter you will see:
*'nohup: appending output to 'nohup.out'*
Now hit enter again to get the command line back.

Once you want to stop the capture, run:
*'ps aux | grep tcpdump'*
and get the process ID for the rolling capture, then run
*'kill -9 processID'*
to stop the rolling capture.

# Secure Web Gateway Troubleshooting - Tcpdump & Network Tools - cont

### Helpful Filters in Wireshark

Request methods (GET – POST – HEAD)

http.request.method == GET

URL-Search

http.request.uri contains "bbc.co.uk"

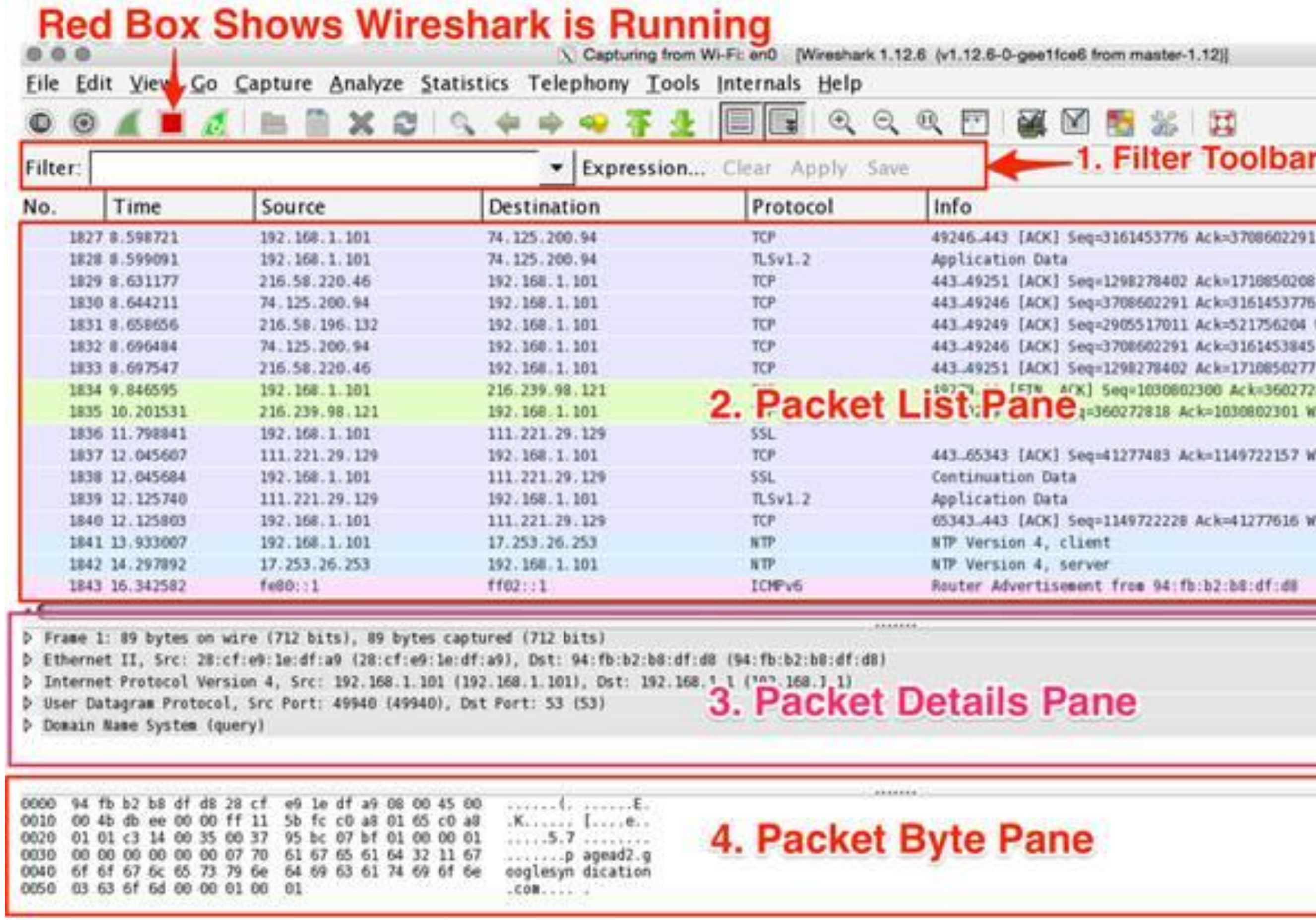
DNS Requests with no Response:

!dns.response_in && dns.flags.response == 0

Filter for protocols

ip.proto eq 253 (cluster comm.)

vrrp; dns



Red Box Shows Wireshark is Running

1. Filter Toolbar

2. Packet List Pane

3. Packet Details Pane

4. Packet Byte Pane

```
Capturing from Wi-Fi: en0   [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
```

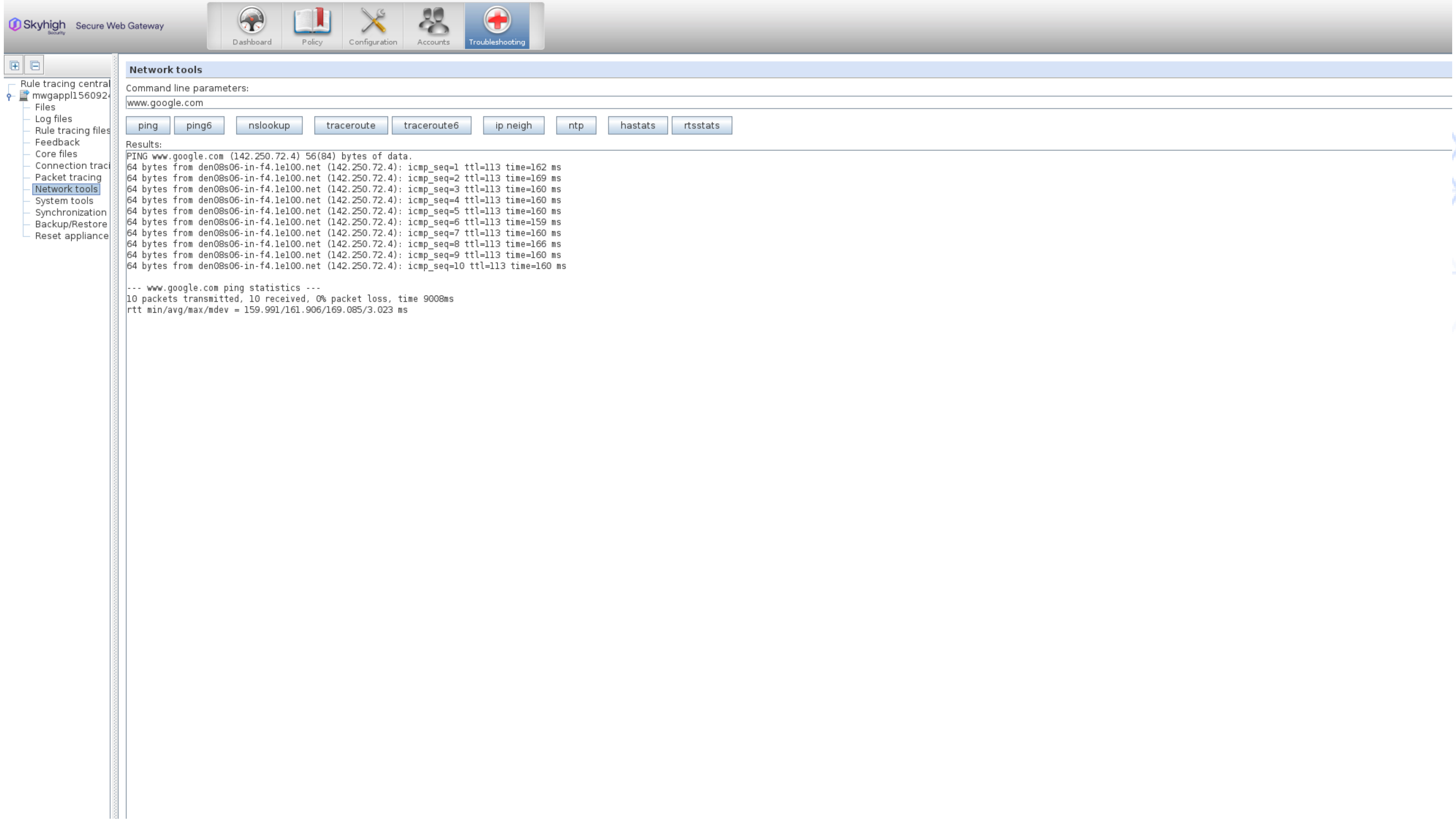
```
No.     Time       Source          Destination     Protocol  Info
   1827 8.598721   192.168.1.101   74.125.200.94   TCP       49246→443 [ACK] Seq=3161453776 Ack=3708602291
   1828 8.599091   192.168.1.101   74.125.200.94   TLSv1.2   Application Data
   1829 8.631177   216.58.220.46   192.168.1.101   TCP       443→49251 [ACK] Seq=1298278402 Ack=1710850208
   1830 8.644211   74.125.200.94   192.168.1.101   TCP       443→49246 [ACK] Seq=3708602291 Ack=3161453776
   1831 8.658656   216.58.196.132  192.168.1.101   TCP       443→49249 [ACK] Seq=2905517011 Ack=521756204
   1832 8.696484   74.125.200.94   192.168.1.101   TCP       443→49246 [ACK] Seq=3708602291 Ack=3161453845
   1833 8.697547   216.58.220.46   192.168.1.101   TCP       443→49251 [ACK] Seq=1298278402 Ack=1710850277
   1834 9.846595   192.168.1.101   216.239.98.121            [FIN, ACK] Seq=1030802300 Ack=360272
   1835 10.201531  216.239.98.121  192.168.1.101             =360272818 Ack=1030802301 W
   1836 11.798841  192.168.1.101   111.221.29.129  SSL
   1837 12.045607  111.221.29.129  192.168.1.101   TCP       443→65343 [ACK] Seq=4127483 Ack=1149722157 W
   1838 12.045684  192.168.1.101   111.221.29.129  SSL       Continuation Data
   1839 12.125740  111.221.29.129  192.168.1.101   TLSv1.2   Application Data
   1840 12.125803  192.168.1.101   111.221.29.129  TCP       65343→443 [ACK] Seq=1149722228 Ack=4127616 W
   1841 13.933007  192.168.1.101   17.253.26.253   NTP       NTP Version 4, client
   1842 14.297892  17.253.26.253   192.168.1.101   NTP       NTP Version 4, server
   1843 16.342582  fe80::1         ff02::1         ICMPv6    Router Advertisement from 94:fb:b2:b8:df:d8
```

```
▷ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
▷ Ethernet II, Src: 28:cf:e9:1e:df:a9 (28:cf:e9:1e:df:a9), Dst: 94:fb:b2:b8:df:d8 (94:fb:b2:b8:df:d8)
▷ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 192.168.1.1 (192.168.1.1)
▷ User Datagram Protocol, Src Port: 49940 (49940), Dst Port: 53 (53)
▷ Domain Name System (query)
```

```
0000  94 fb b2 b8 df d8 28 cf  e9 1e df a9 08 00 45 00   ......(. ......E.
0010  00 4b db ee 00 00 ff 11  5b fc c0 a8 01 65 c0 a8   .K...... [....e..
0020  01 01 c3 14 00 35 00 37  95 bc 07 bf 01 00 00 01   .....5.7 ........
0030  00 00 00 00 00 00 07 70  61 67 65 61 64 32 11 67   .......p agead2.g
0040  6f 6f 67 6c 65 73 79 6e  64 69 63 61 74 69 6f 6e   ooglesyn dication
0050  03 63 6f 6d 00 00 01 00  01                        .com.... .
```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

# Secure Web Gateway Troubleshooting - Tcpdump & Network Tools



Command line parameters: www.google.com

Results:

```
PING www.google.com (142.250.72.4) 56(84) bytes of data.
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=1 ttl=113 time=162 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=2 ttl=113 time=169 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=3 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=4 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=5 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=6 ttl=113 time=159 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=7 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=8 ttl=113 time=166 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=9 ttl=113 time=160 ms
64 bytes from den08s06-in-f4.1e100.net (142.250.72.4): icmp_seq=10 ttl=113 time=160 ms

--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008ms
rtt min/avg/max/mdev = 159.991/161.906/169.085/3.023 ms
```

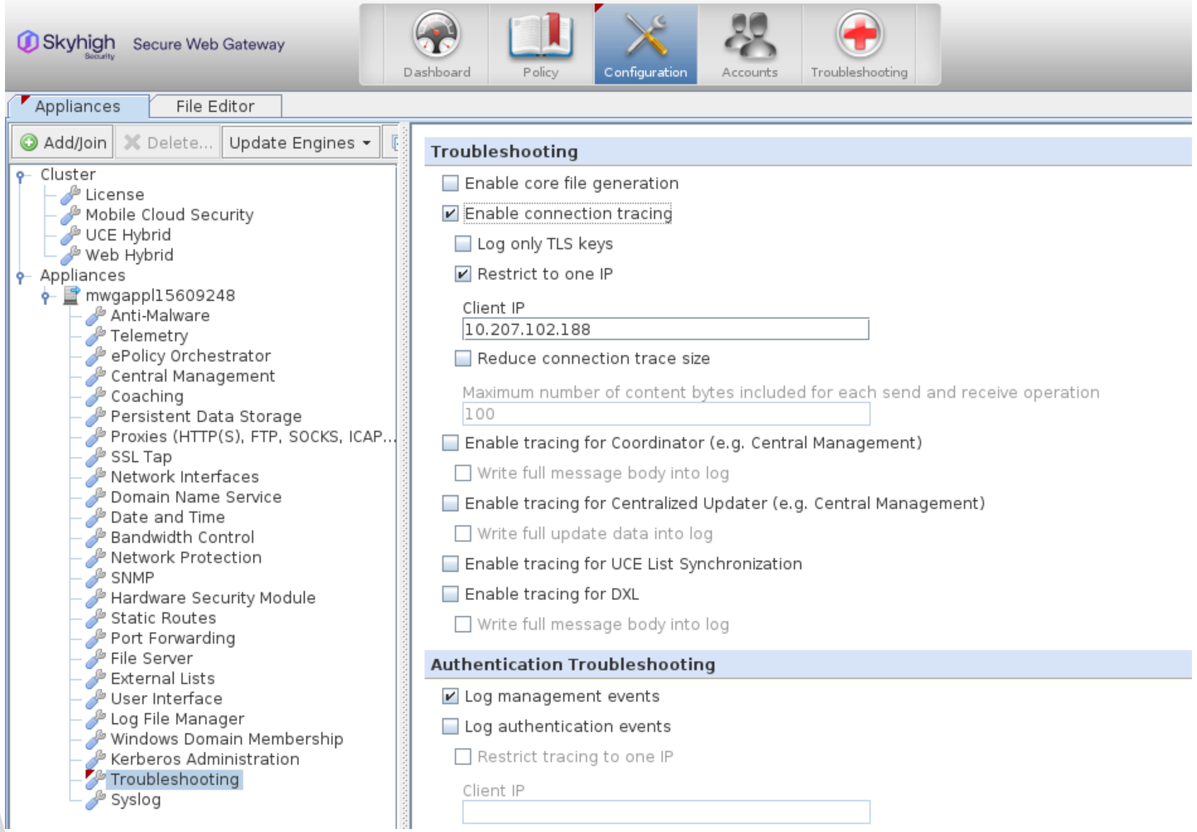
# Secure Web Gateway Troubleshooting – Connection Traces

In HTTP communication is sent in clear text but in HTTPS all communication is encrypted.

Connection Traces in the most basic term turns encrypted into plain text.

Support will often ask for connection traces when facing issues with HTTPs sites

**NOTE**: SSL Scanning has to be enabled in order to decrypt the complete traffic



**Troubleshooting**

☐ Enable core file generation

☑ Enable connection tracing

☐ Log only TLS keys

☑ Restrict to one IP

Client IP: 10.207.102.188

☐ Reduce connection trace size

Maximum number of content bytes included for each send and receive operation: 100

☐ Enable tracing for Coordinator (e.g. Central Management)

☐ Write full message body into log

☐ Enable tracing for Centralized Updater (e.g. Central Management)

☐ Write full update data into log

☐ Enable tracing for UCE List Synchronization

☐ Enable tracing for DXL

☐ Write full message body into log

**Authentication Troubleshooting**

☑ Log management events

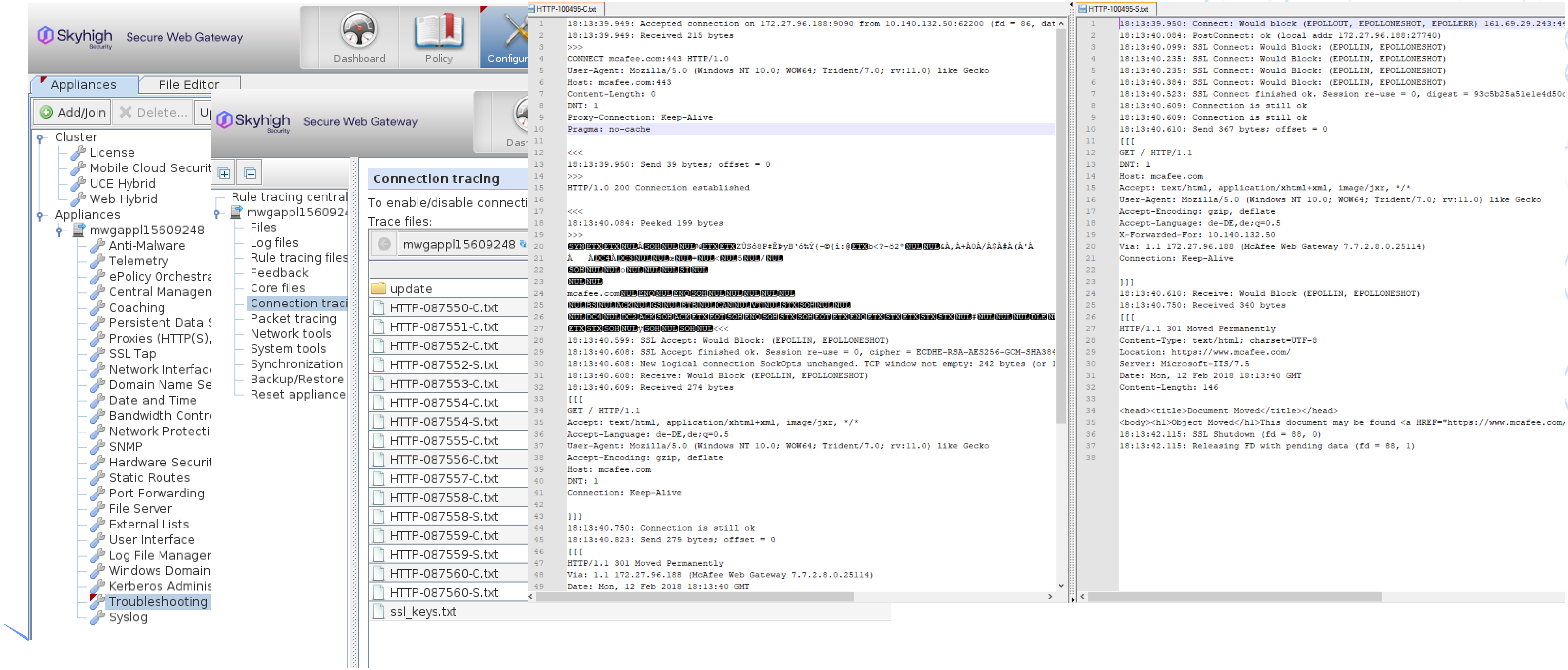
☐ Log authentication events

☐ Restrict tracing to one IP

Client IP:

# Secure Web Gateway Troubleshooting – Connection Traces - Cont

Configuration -> Troubleshooting > Connection Tracing



HTTP-100495-C.txt

```
18:13:39.949: Accepted connection on 172.27.96.188:9090 from 10.140.132.50:62200 (fd = 86, dat
18:13:39.949: Received 215 bytes
>>>
CONNECT mcafee.com:443 HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: mcafee.com:443
Content-Length: 0
DNT: 1
Proxy-Connection: Keep-Alive
Pragma: no-cache

<<<
18:13:39.950: Send 39 bytes; offset = 0
>>>
HTTP/1.0 200 Connection established

<<<
18:13:40.084: Peeked 199 bytes
>>>
SYNETXETXNULÂSOHNULNUL¾ETXETXZÙSô8P‡ÊÞyB'ó‰Ý{-©{î:@ETXb<?-ö2°NULNUL&À,À+À0À/À$À#À(À'À
À   ÀDC4ÀDC3NULNULœNUL=NUL<NUL5NUL/NUL
SOHNULNULoNULNULNULSINUL
NULNUL
mcafee.comNULENQNULENQSOHNULNULNULNULNUL
NULBSNULACKNULGSNULETBNULCANNULVTNULSTXSOHNULNUL
NULDC4NULDC2ACKSOHACKETXEOTSOHENQSOHSTXSOHEOTETXENQETXSTXETXSTXSTXNUL#NULNULNULDLEN
ETXSTXSOHNULÿSOHNULSOHNUL<<<
18:13:40.599: SSL Accept: Would Block: (EPOLLIN, EPOLLONESHOT)
18:13:40.608: SSL Accept finished ok. Session re-use = 0, cipher = ECDHE-RSA-AES256-GCM-SHA384
18:13:40.608: New logical connection SockOpts unchanged. TCP window not empty: 242 bytes (or 1
18:13:40.608: Receive: Would Block (EPOLLIN, EPOLLONESHOT)
18:13:40.609: Received 274 bytes
[[[
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: de-DE,de;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: mcafee.com
DNT: 1
Connection: Keep-Alive

]]]
18:13:40.750: Connection is still ok
18:13:40.823: Send 279 bytes; offset = 0
[[[
HTTP/1.1 301 Moved Permanently
Via: 1.1 172.27.96.188 (McAfee Web Gateway 7.7.2.8.0.25114)
Date: Mon, 12 Feb 2018 18:13:40 GMT
```

HTTP-100495-S.txt

```
18:13:39.950: Connect: Would block (EPOLLOUT, EPOLLONESHOT, EPOLLERR) 161.69.29.243:44
18:13:40.084: PostConnect: ok (local addr 172.27.96.188:27740)
18:13:40.099: SSL Connect: Would Block: (EPOLLIN, EPOLLONESHOT)
18:13:40.235: SSL Connect: Would Block: (EPOLLIN, EPOLLONESHOT)
18:13:40.235: SSL Connect: Would Block: (EPOLLIN, EPOLLONESHOT)
18:13:40.384: SSL Connect: Would Block: (EPOLLIN, EPOLLONESHOT)
18:13:40.523: SSL Connect finished ok. Session re-use = 0, digest = 93c5b25a51e1e4d50c
18:13:40.609: Connection is still ok
18:13:40.609: Connection is still ok
18:13:40.610: Send 367 bytes; offset = 0
[[[
GET / HTTP/1.1
DNT: 1
Host: mcafee.com
Accept: text/html, application/xhtml+xml, image/jxr, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.5
X-Forwarded-For: 10.140.132.50
Via: 1.1 172.27.96.188 (McAfee Web Gateway 7.7.2.8.0.25114)
Connection: Keep-Alive

]]]
18:13:40.610: Receive: Would Block (EPOLLIN, EPOLLONESHOT)
18:13:40.750: Received 340 bytes
[[[
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: https://www.mcafee.com/
Server: Microsoft-IIS/7.5
Date: Mon, 12 Feb 2018 18:13:40 GMT
Content-Length: 146

<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a HREF="https://www.mcafee.com/
18:13:42.115: SSL Shutdown (fd = 88, 0)
18:13:42.115: Releasing FD with pending data (fd = 88, 1)
```

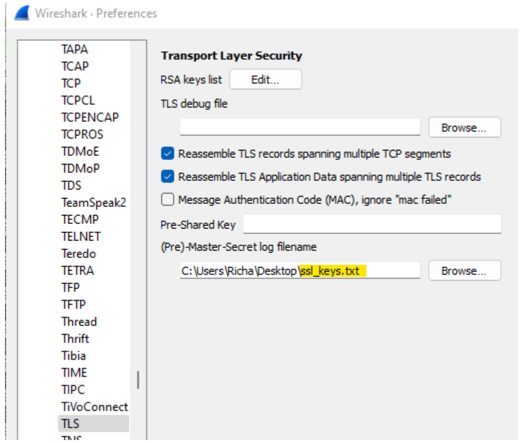
# Secure Web Gateway Troubleshooting – Connection Traces
# Decrypt SSL with Keys from Connection Trace

## Take aways:

- If you see what looks like junk do not worry this is typically HTTP2 this would be accepted at support as we can decode this:

16:15:23.624: Send 27 bytes
unsigned char send_1[] = { 0x00, 0x00, 0x12, 0x04, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x03, 0x00, 0x00, 0x00, 0x64, 0x00, 0x06, 0x00, 0x00, 0x80, 0x00 }; // { SETTINGS: stream = 0, len = 18, flags = 0 }.

- Connection traces will trace from the client in the '-C' file and from the proxy to the destination in the '-S' file.
- From support we would need the TCP dump started first then the connection traces started with the ssl_keys file so we can decode the TCP dump streams.
- Will often be request by support for issues with websites/web applications.
- To decode TCP dump using the ssl keys:



Transport Layer Security

RSA keys list

TLS debug file

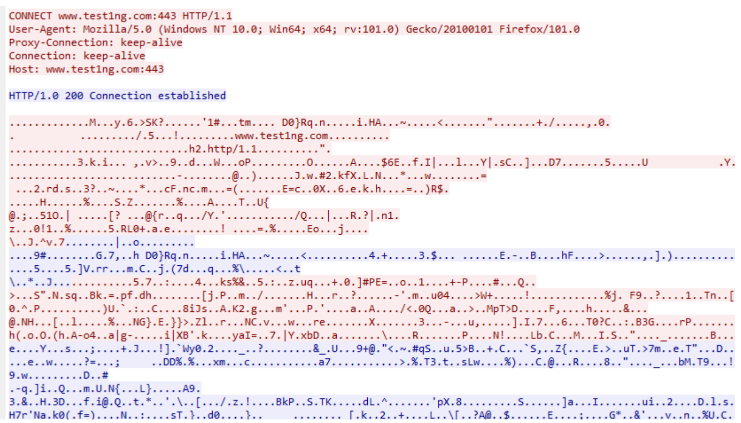
☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS records

☐ Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared Key

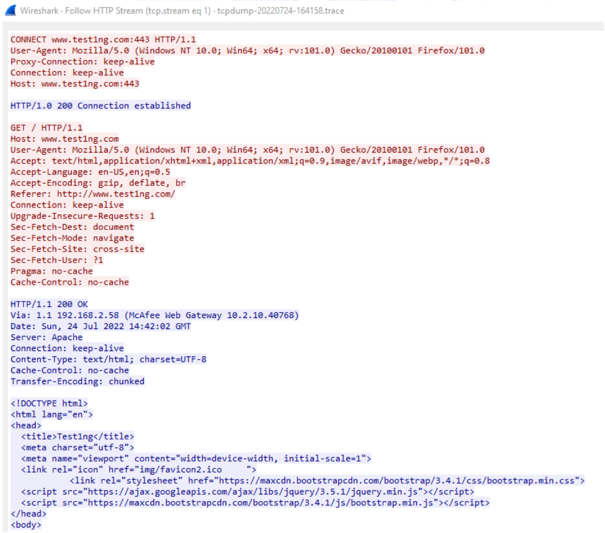
(Pre)-Master-Secret log filename: C:\Users\Richa\Desktop\ssl_keys.txt



```
CONNECT www.test1ng.com:443 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Proxy-Connection: keep-alive
Connection: keep-alive
Host: www.test1ng.com:443

HTTP/1.0 200 Connection established

............M...y.6.>SK?......'1#...tm.... D0}Rq.n.....i.HA...~.....<......."......+./.....,.0.
.          ........./.5...!........www.test1ng.com..........
...........................h2.http/1.1.........".
..........3.k.i... ,.v>..9..d...W...oP.........O......A....$6E..f.I|...l...Y|.sC..]...D7.......5.....U        .Y.
..........................-........@..)......J.w.#2.kfX.L.N...*...w........=
 ...2.rd.s..3?..~....*...cF.nc.m...=(.......E=c..0X..6.e.k.h....=..)R$.
.....H......%....S.Z.......%....A....T..U{
@.;..51O.| .....[? ...@{r..q.../Y.'.........../Q...|...R.?|.n1.
z...0!1..%......5.RL0+.a.e........! ....=.%.....Eo...j....
\..J.^v.7........|..o.........
....9#........G.7,..h D0}Rq.n.....i.HA...~.....<..........4.+.....3.$... ......E.-..B....hF....>......,.].).........
....5....5.]V.rr...m.C..j.(7d...q...%\.....<..t
\..*..J............5.7..:....4...ks%&..5.:..z.uq...+.0.]#PE=..o..1....+-P....#...Q..
>...S".N.sq..Bk.=.pf.dh........[j.P..m../.......H...r..?......-'.m..u04....>W+.....!...........%j. F9..?....1..Tn..[
0.^.P..........)U.`.:..C....8iJs..A.K2.g...m'...P.'....a..A..../<.0Q...a..>..MpT>D.....F,....h.....&...
@.NH...[..l.....%...NG}.E.}}>.Zl..r...NC.v...w...re.......X.......3...-...u,.....].I.7...6...T0?C..:.B3G....rP.......
h(.o.O.(h.A-o4..a|g-.....i|XB'.k....yaI=..7.|Y.xbD..a.......\....R.......P....N!....Lb.C...M...I.S..".._......B...
e....Y...s...;....+.J...!].`Wy0.2...._..?........&_.U...9+@."<.~.#qS..u.5>B..+.C...`S,..Z{....E.>..uT.>7m..e.T"...D..
...e..w.....?=...;     ..DD%.%...xm...c...........a7...........>.%.T3.t..sLw....%)...C.@...R....8.."...._...bM.T9...!
9.w.........D..#
.-q.]i..Q...m.U.N{...L}.....A9.
3.&..H.3D...f.i@.Q..t.*..'.\..[.../.z.!....BkP..S.TK.....dL.^.......'pX.8.........S......]a...I.......ui..2....D.l.s.
H7r'Na.k0(.f=)....N..:....sT.}..d0....}..    ........[.k..2..+....L..\[..?A@..$......E....;....G*..&'...v..n..%U.C.
```


Wireshark · Follow HTTP Stream (tcp.stream eq 1) · tcpdump-20220724-164158.trace

```
CONNECT www.test1ng.com:443 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Proxy-Connection: keep-alive
Connection: keep-alive
Host: www.test1ng.com:443

HTTP/1.0 200 Connection established

GET / HTTP/1.1
Host: www.test1ng.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://www.test1ng.com/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Via: 1.1 192.168.2.58 (McAfee Web Gateway 10.2.10.40768)
Date: Sun, 24 Jul 2022 14:42:02 GMT
Server: Apache
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Cache-Control: no-cache
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="en">
<head>
  <title>Test1ng</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="icon" href="img/favicon2.ico     ">
           <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/css/bootstrap.min.css">
  <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
  <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js"></script>
</head>
<body>
```

# Secure Web Gateway Troubleshooting – Connection Traces

**Reading of Connection Traces**

Each entry in the traces begins with a timestamp of when the entry was written. Here is a table of possible log entries

| | |
|---|---|
| Connect: Would block (EPOLLOUT, EPOLLONESHOT, EPOLLERR) :80 IP = "10.150.97.74" | SWG initiated a connect call to 10.15.97.74 on port 80. Depending on the context there could also be a FQDM before the port (a SYN package was sent) |
| Connected transparently to :80 IP = "10.150.97.74" | SWG is running in bridge or router mode, has IP spoofing enabled and cloned a connection |
| Connection – using existing connection – to :80 IP = "10.150.97.74" | SWG uses an already connected socket for this connection |
| PostConnect: <status> | The TCP handshake has finished and the status of the connection is <status> |
| Connection is still ok | SWG verified if the connection is ok (will be used for example to detect dead clients) and it is ok |
| Connection is already dead / Connection isn’t ok | SWG verified if the connection is ok and it isn’t ok |
| Send <n> bytes <brackets> <data> <brackets> | SWG has sent data. The brackets are a “<<<” – “>>>” or a “[]” pair. The first pair indicates plain text data where as the second pair will be used for SSL encrypted traffic. |
| Received <n> bytes <brackets> <data> <brackets> | The same as above (only receive) |
| Sent: Would Block (EPOLLIN, EPOLLONESHOT) | SWG wanted to send data, but the kernel was not yet willing to accept it. This is not an error. |
| Receive: Would Block (EPOLLIN, EPOLLONESHOT) | SWG wanted to read data from a socket, but there was no data. This is not an error. |
| Accepted connection on <MWG IP>:<ProxyPort> from <ClientIP>:<ClientPort> | SWG has accepted a connection. The local (proxy) port will be given as well as the client IP address and port. |
| Connection has received FIN | The peer has closed the connection. |
| SSL Shutdown | SWG terminates the SSL (not the TCP!) connection. |
| Releasing FD but keep it open | SWG removes the socket from this connection but keeps it open for later reuse. |
| Releasing and closing FD | SWG removes the socket from this connections and closes it. |

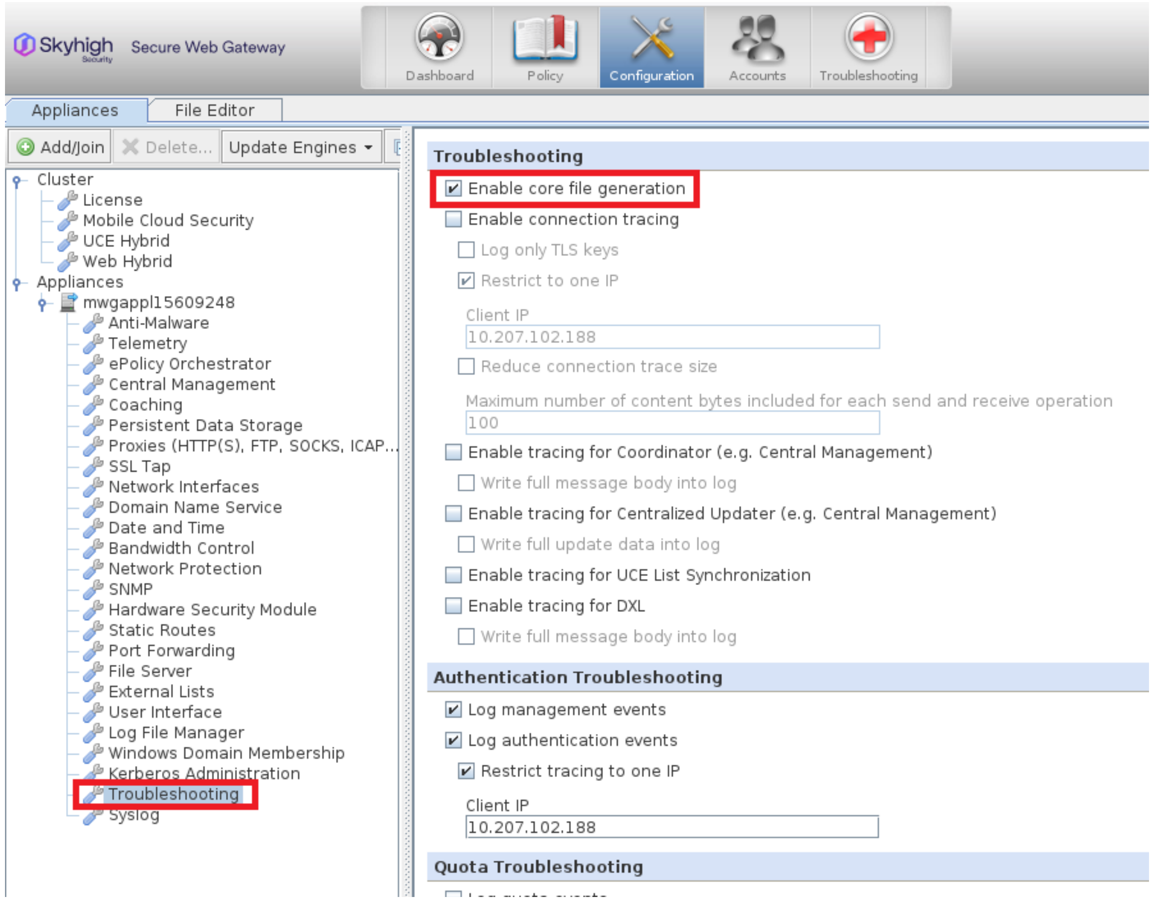
# Secure Web Gateway Troubleshooting – Core Dump

High CPU

High Memory / Memory Leak

Crashes / Services / Server

Created core files can be found in:
Troubleshooting > Core files



**Troubleshooting**

☑ Enable core file generation

☐ Enable connection tracing

☐ Log only TLS keys

☑ Restrict to one IP

Client IP
10.207.102.188

☐ Reduce connection trace size

Maximum number of content bytes included for each send and receive operation
100

☐ Enable tracing for Coordinator (e.g. Central Management)

☐ Write full message body into log

☐ Enable tracing for Centralized Updater (e.g. Central Management)

☐ Write full update data into log

☐ Enable tracing for UCE List Synchronization

☐ Enable tracing for DXL

☐ Write full message body into log

**Authentication Troubleshooting**

☑ Log management events

☑ Log authentication events

☑ Restrict tracing to one IP

Client IP
10.207.102.188

**Quota Troubleshooting**

# Secure Web Gateway Troubleshooting – Core Dump - Cont

If you need to manually trigger a core dump this can be done in various ways. You need to du this during the high CPU or memory issue!

The main dump forced:

Navigate to the cores folder:

```
      # cd /opt/mwg/log/debug/cores
```

Perform the  procedure below:

```
      #  gcore `pgrep -n mwg-core`
```

Check the status of the mwg status':

```
      # service mwg status
```

Verify the core file was created:

```
      # ll
```

Rename the core file to match: [PROCESS-NAME]-[PID].core

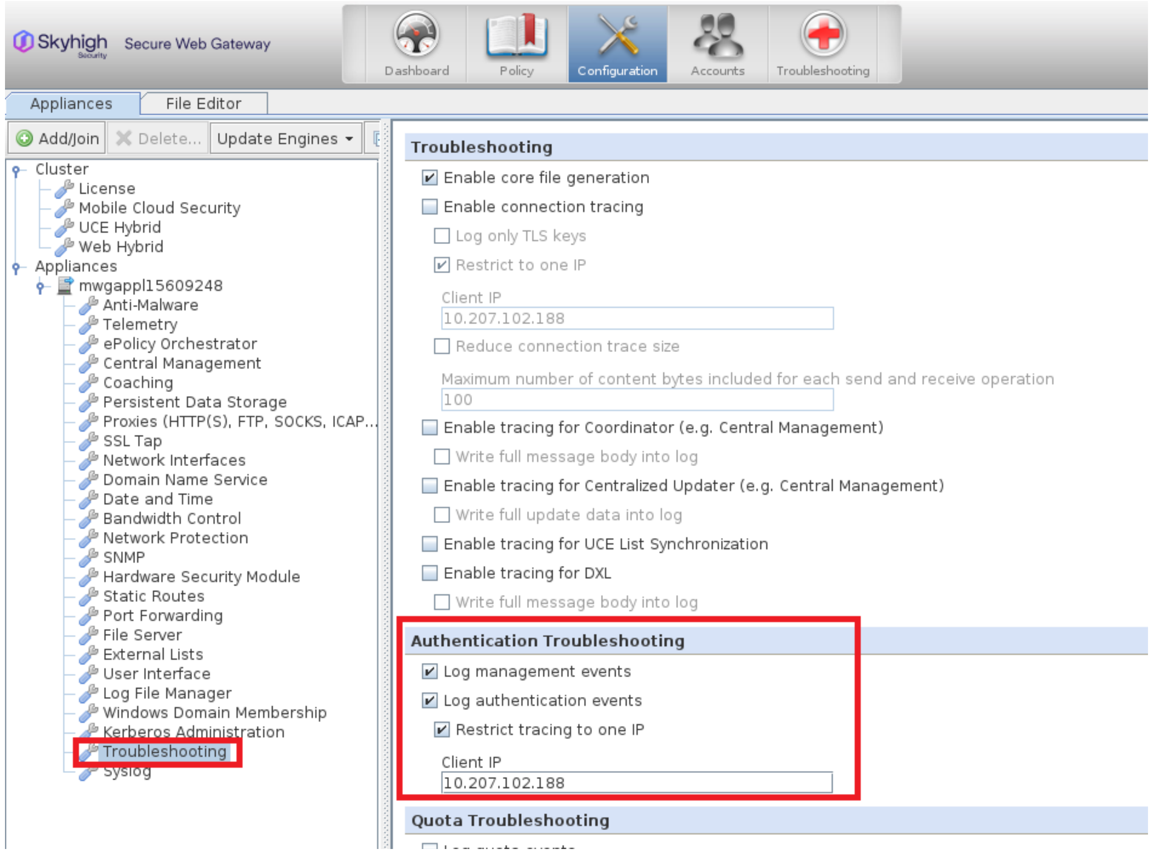
```
      # The format should be something like:
      # mv <nameofcreatedcorefile> mwg-core-3902.core
```

Compress the core file (we use 'gzip -9' in case it is larger than 4GB), substitute '[FILENAME]' with the filename of the desired core file:

```
      # cd /opt/mwg/log/debug/cores
      # gzip -9 [FILENAME]
      # mv [FILENAME].gz
#your_service_request_number#_[FILENAME].gz
```

# Secure Web Gateway Troubleshooting – Authentication

- Authentication Debug logging
- Secure Net logon



**Troubleshooting**

- ☑ Enable core file generation
- ☐ Enable connection tracing
  - ☐ Log only TLS keys
  - ☑ Restrict to one IP
  - Client IP: 10.207.102.188
  - ☐ Reduce connection trace size
  - Maximum number of content bytes included for each send and receive operation: 100
- ☐ Enable tracing for Coordinator (e.g. Central Management)
  - ☐ Write full message body into log
- ☐ Enable tracing for Centralized Updater (e.g. Central Management)
  - ☐ Write full update data into log
- ☐ Enable tracing for UCE List Synchronization
- ☐ Enable tracing for DXL
  - ☐ Write full message body into log

**Authentication Troubleshooting**

- ☑ Log management events
- ☑ Log authentication events
  - ☑ Restrict tracing to one IP
  - Client IP: 10.207.102.188

**Quota Troubleshooting**

# Secure Web Gateway Troubleshooting – Authentication Debug

Log file located > Troubleshooting > Log Files > Debug > „mwg-core__Auth.debug.log “

We can generate some examples of reasons why authentication is not working, here I am looking at NTLM.

User does not exist:

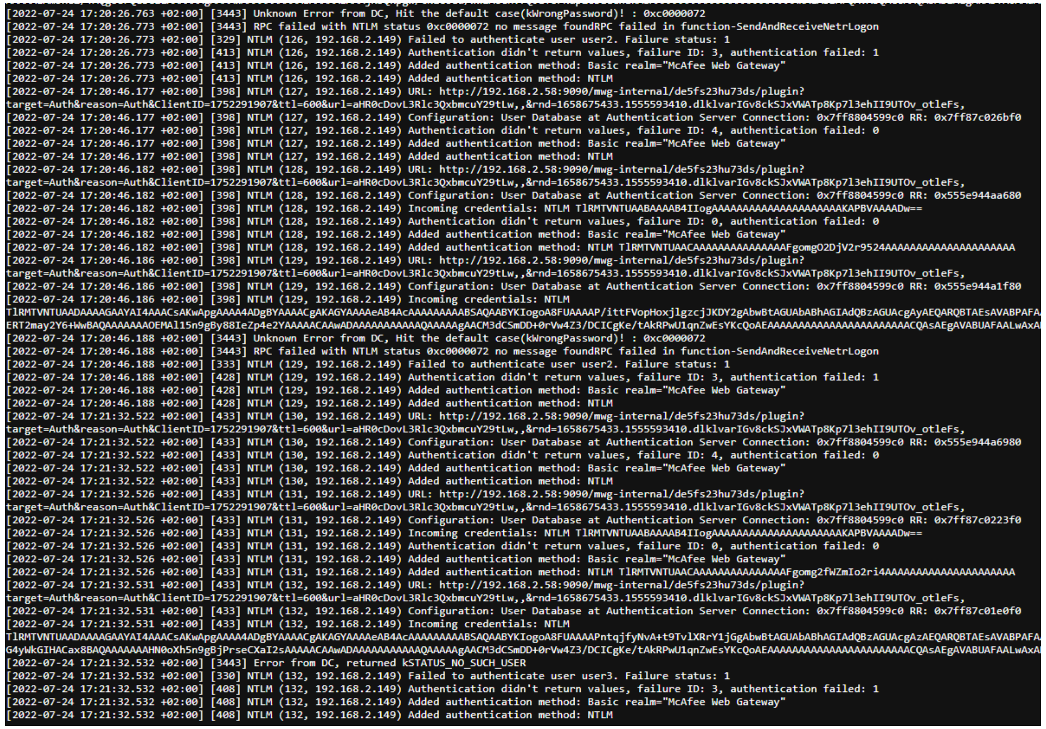
Error from DC, returned kSTATUS_NO_SUCH_USER
Failed to authenticate user user3

User logon with misspelled or bad password:

Unknown Error from DC, Hit the default case(kWrongPassword)! : 0xc000006a
RPC failed with NTLM status 0xc000006a STATUS_WRONG_PASSWORDRPC failed in function-SendAndReceiveNetrLogon

User logon to account disabled by administrator:

Unknown Error from DC, Hit the default case(kWrongPassword)! : 0xc0000072
RPC failed with NTLM status 0xc0000072 no message foundRPC failed in function-SendAndReceiveNetrLogon



```
[2022-07-24 17:20:26.763 +02:00] [3443] Unknown Error from DC, Hit the default case(kWrongPassword)! : 0xc0000072
[2022-07-24 17:20:26.773 +02:00] [3443] RPC failed with NTLM status 0xc0000072 no message foundRPC failed in function-SendAndReceiveNetrLogon
[2022-07-24 17:20:26.773 +02:00] [329] NTLM (126, 192.168.2.149) Failed to authenticate user user2. Failure status: 1
[2022-07-24 17:20:26.773 +02:00] [413] NTLM (126, 192.168.2.149) Authentication didn't return values, failure ID: 3, authentication failed: 1
[2022-07-24 17:20:26.773 +02:00] [413] NTLM (126, 192.168.2.149) Added authentication method: Basic realm="McAfee Web Gateway"
[2022-07-24 17:20:26.773 +02:00] [413] NTLM (126, 192.168.2.149) Added authentication method: NTLM
[2022-07-24 17:20:46.177 +02:00] [398] NTLM (127, 192.168.2.149) URL: http://192.168.2.58:9090/mwg-internal/de5fs23hu73ds/plugin?
target=Auth&reason=Auth&ClientID=1752291907&ttl=600&url=aHR0cDovL3Rlc3QxbmcuY29tLw,,&rnd=1658675433.1555593410.dlklvarIGv8ckSJxVWATp8Kp7l3ehII9UTOv_otleFs,
[2022-07-24 17:20:46.177 +02:00] [398] NTLM (127, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff8804599c0 RR: 0x7ff87c026bf0
[2022-07-24 17:20:46.177 +02:00] [398] NTLM (127, 192.168.2.149) Authentication didn't return values, failure ID: 4, authentication failed: 0
[2022-07-24 17:20:46.177 +02:00] [398] NTLM (127, 192.168.2.149) Added authentication method: Basic realm="McAfee Web Gateway"
[2022-07-24 17:20:46.177 +02:00] [398] NTLM (127, 192.168.2.149) Added authentication method: NTLM
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) URL: http://192.168.2.58:9090/mwg-internal/de5fs23hu73ds/plugin?
target=Auth&reason=Auth&ClientID=1752291907&ttl=600&url=aHR0cDovL3Rlc3QxbmcuY29tLw,,&rnd=1658675433.1555593410.dlklvarIGv8ckSJxVWATp8Kp7l3ehII9UTOv_otleFs,
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff8804599c0 RR: 0x555e944aa680
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) Incoming credentials: NTLM TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAAAAAAAAAKAPBVAAAADw==
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) Authentication didn't return values, failure ID: 0, authentication failed: 0
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) Added authentication method: Basic realm="McAfee Web Gateway"
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) Added authentication method: NTLM TlRMTVNTUAACAAAAAAAAAAAAAAAAFgomgO2DjV2r9524AAAAAAAAAAAAAAAAAAAA
[2022-07-24 17:20:46.186 +02:00] [398] NTLM (129, 192.168.2.149) URL: http://192.168.2.58:9090/mwg-internal/de5fs23hu73ds/plugin?
target=Auth&reason=Auth&ClientID=1752291907&ttl=600&url=aHR0cDovL3Rlc3QxbmcuY29tLw,,&rnd=1658675433.1555593410.dlklvarIGv8ckSJxVWATp8Kp7l3ehII9UTOv_otleFs,
[2022-07-24 17:20:46.186 +02:00] [398] NTLM (129, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff8804599c0 RR: 0x555e944a1f80
[2022-07-24 17:20:46.186 +02:00] [398] NTLM (129, 192.168.2.149) Incoming credentials: NTLM
TlRMTVNTUAADAAAAGAAYAI4AAACsAKwApgAAAA4ADgBYAAAACgAKAGYAAAAeAB4AcAAAAAAAAABSAQAABYKIogoA8FUAAAAP/ittFVopHoxjlgzcjJKDY2gAbwBtAGUAbABhAGIAdQBzAGUAcgAyAEQARQBTAEsAVABPAFA
ERT2may2Y6+WwBAQAAAAAAAOEMAl15n9gBy88IeZp4e2YAAAAACAAwADAAAAAAAAAAAQAAAAAgAACM3dCSmDD+0rVw4Z3/DCICgKe/tAkRPwU1qnZwEsYKcQoAEAAAAAAAAAAAAAAAAAAAAAAAACQAsAEgAVABUAFAALwAxA
[2022-07-24 17:20:46.188 +02:00] [3443] Unknown Error from DC, Hit the default case(kWrongPassword)! : 0xc0000072
[2022-07-24 17:20:46.188 +02:00] [3443] RPC failed with NTLM status 0xc0000072 no message foundRPC failed in function-SendAndReceiveNetrLogon
[2022-07-24 17:20:46.188 +02:00] [333] NTLM (129, 192.168.2.149) Failed to authenticate user user2. Failure status: 1
[2022-07-24 17:20:46.188 +02:00] [428] NTLM (129, 192.168.2.149) Authentication didn't return values, failure ID: 3, authentication failed: 1
[2022-07-24 17:20:46.188 +02:00] [428] NTLM (129, 192.168.2.149) Added authentication method: Basic realm="McAfee Web Gateway"
[2022-07-24 17:20:46.188 +02:00] [428] NTLM (129, 192.168.2.149) Added authentication method: NTLM
[2022-07-24 17:21:32.522 +02:00] [433] NTLM (130, 192.168.2.149) URL: http://192.168.2.58:9090/mwg-internal/de5fs23hu73ds/plugin?
target=Auth&reason=Auth&ClientID=1752291907&ttl=600&url=aHR0cDovL3Rlc3QxbmcuY29tLw,,&rnd=1658675433.1555593410.dlklvarIGv8ckSJxVWATp8Kp7l3ehII9UTOv_otleFs,
[2022-07-24 17:21:32.522 +02:00] [433] NTLM (130, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff8804599c0 RR: 0x555e944a6980
[2022-07-24 17:21:32.522 +02:00] [433] NTLM (130, 192.168.2.149) Authentication didn't return values, failure ID: 4, authentication failed: 0
[2022-07-24 17:21:32.522 +02:00] [433] NTLM (130, 192.168.2.149) Added authentication method: Basic realm="McAfee Web Gateway"
[2022-07-24 17:21:32.522 +02:00] [433] NTLM (130, 192.168.2.149) Added authentication method: NTLM
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) URL: http://192.168.2.58:9090/mwg-internal/de5fs23hu73ds/plugin?
target=Auth&reason=Auth&ClientID=1752291907&ttl=600&url=aHR0cDovL3Rlc3QxbmcuY29tLw,,&rnd=1658675433.1555593410.dlklvarIGv8ckSJxVWATp8Kp7l3ehII9UTOv_otleFs,
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff8804599c0 RR: 0x7ff87c0223f0
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) Incoming credentials: NTLM TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAAAAAAAAAKAPBVAAAADw==
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) Authentication didn't return values, failure ID: 0, authentication failed: 0
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) Added authentication method: Basic realm="McAfee Web Gateway"
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) Added authentication method: NTLM TlRMTVNTUAACAAAAAAAAAAAAAAAAFgomg2fWZmIo2ri4AAAAAAAAAAAAAAAAAAAA
[2022-07-24 17:21:32.531 +02:00] [433] NTLM (132, 192.168.2.149) URL: http://192.168.2.58:9090/mwg-internal/de5fs23hu73ds/plugin?
target=Auth&reason=Auth&ClientID=1752291907&ttl=600&url=aHR0cDovL3Rlc3QxbmcuY29tLw,,&rnd=1658675433.1555593410.dlklvarIGv8ckSJxVWATp8Kp7l3ehII9UTOv_otleFs,
[2022-07-24 17:21:32.531 +02:00] [433] NTLM (132, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff8804599c0 RR: 0x7ff87c01e0f0
[2022-07-24 17:21:32.531 +02:00] [433] NTLM (132, 192.168.2.149) Incoming credentials: NTLM
TlRMTVNTUAADAAAAGAAYAI4AAACsAKwApgAAAA4ADgBYAAAACgAKAGYAAAAeAB4AcAAAAAAAAABSAQAABYKIogoA8FUAAAAPntqjfyNvA+t9TvlXRrY1jGgAbwBtAGUAbABhAGIAdQBzAGUAcgAzAEQARQBTAEsAVABPAFA
G4yWkGIHACax8BAQAAAAAAAHN0oXh5n9gBjPrseCXaI2sAAAAACAAwADAAAAAAAAAAAQAAAAAgAACM3dCSmDD+0rVw4Z3/DCICgKe/tAkRPwU1qnZwEsYKcQoAEAAAAAAAAAAAAAAAAAAAAAAAACQAsAEgAVABUAFAALwAxA
[2022-07-24 17:21:32.532 +02:00] [3443] Error from DC, returned kSTATUS_NO_SUCH_USER
[2022-07-24 17:21:32.532 +02:00] [330] NTLM (132, 192.168.2.149) Failed to authenticate user user3. Failure status: 1
[2022-07-24 17:21:32.532 +02:00] [408] NTLM (132, 192.168.2.149) Authentication didn't return values, failure ID: 3, authentication failed: 1
[2022-07-24 17:21:32.532 +02:00] [408] NTLM (132, 192.168.2.149) Added authentication method: Basic realm="McAfee Web Gateway"
[2022-07-24 17:21:32.532 +02:00] [408] NTLM (132, 192.168.2.149) Added authentication method: NTLM
```

| Status\Sub-Status Code | Description |
|---|---|
| 0XC000005E | There are currently no logon servers available to service the logon request. |
| 0xC0000064 | User logon with misspelled or bad user account |
| 0xC000006A | User logon with misspelled or bad password |
| 0XC000006D | The cause is either a bad username or authentication information |
| 0XC000006E | Indicates a referenced user name and authentication information are valid, but some user account restriction has prevented successful authentication (such as time-of-day restrictions). |
| 0xC000006F | User logon outside authorized hours |
| 0xC0000070 | User logon from unauthorized workstation |
| 0xC0000071 | User logon with expired password |
| 0xC0000072 | User logon to account disabled by administrator |
| 0XC00000DC | Indicates the Sam Server was in the wrong state to perform the desired operation. |
| 0XC0000133 | Clocks between DC and other computer too far out of sync |
| 0XC000015B | The user has not been granted the requested logon type (also called the *logon right*) at this machine |
| 0XC000018C | The logon request failed because the trust relationship between the primary domain and the trusted domain failed. |
| 0XC0000192 | An attempt was made to logon, but the **Netlogon** service was not started. |
| 0xC0000193 | User logon with expired account |
| 0XC0000224 | User is required to change password at next logon |
| 0XC0000225 | Evidently a bug in Windows and not a risk |
| 0xC0000234 | User logon with account locked |
| 0XC00002EE | Failure Reason: An Error occurred during Logon |
| 0XC0000413 | Logon Failure: The machine you are logging on to is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine. |
| 0x0 | Status OK. |

# Secure Web Gateway Troubleshooting – Authentication Debug - cont

Secure Net logon

In conjunction with the auth debug logs we now also sometimes need the Netlogon Logs.

Webgateway commincates via port 445 but with secure all we now see is blob data so no request or responce is in clear text.

Netlogon Logs will record the request and responce but this is done on Windows Server itself:

https://docs.microsoft.com/en-us/troubleshoot/windows-client/windows-security/enable-debug-logging-netlogon-service

# Secure Web Gateway Troubleshooting – Authentication Debug - cont

## Secure Net logon

Enable with admin cmd prompt:

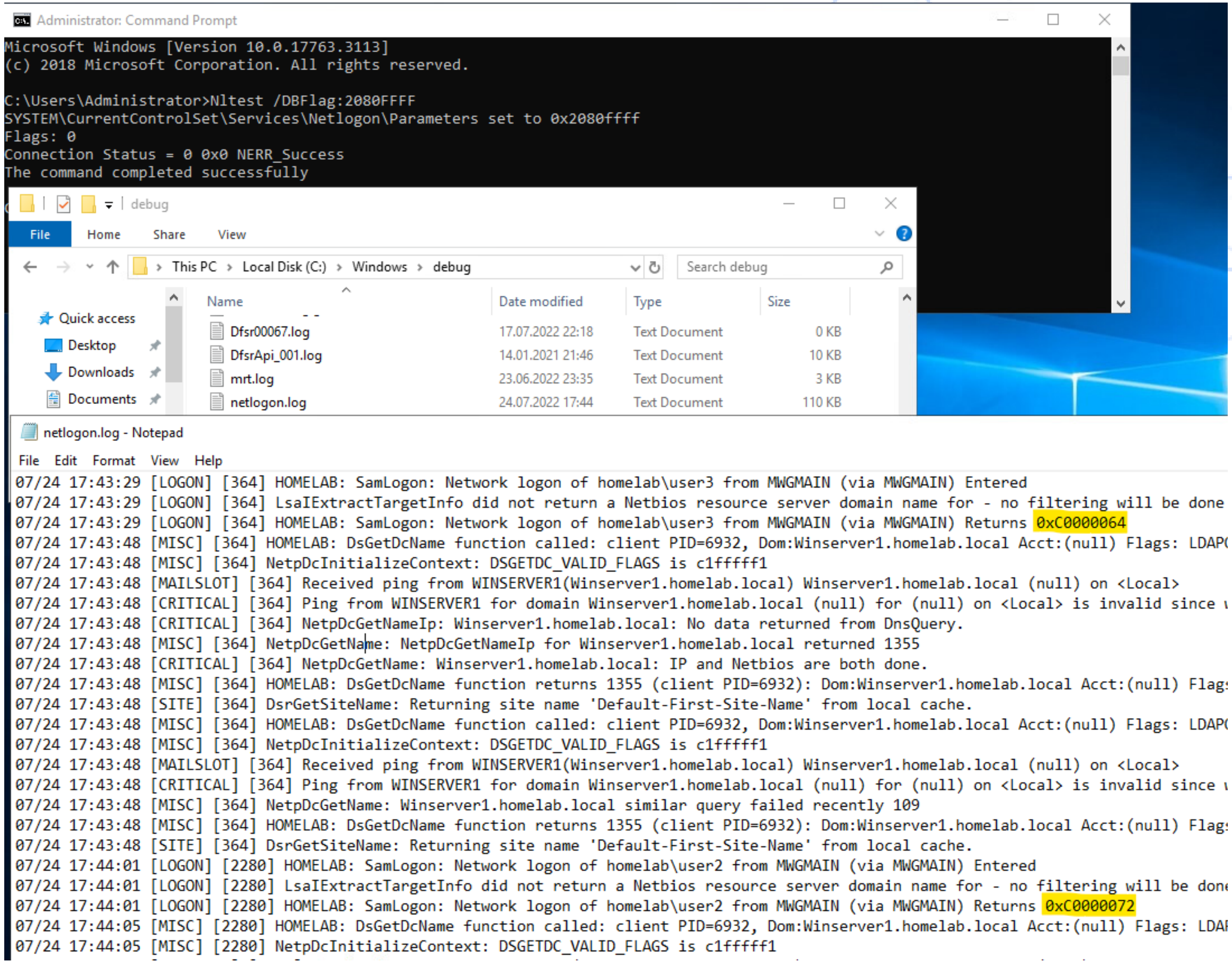
Nltest /DBFlag:2080FFFF

Disable with admin cmd prompt:

Nltest /DBFlag:0x0

Log can be found:

C Drive > Windows > Debug


Administrator: Command Prompt
debug
File
Home
Share
View
This PC › Local Disk (C:) › Windows › debug
Search debug
Quick access
Desktop
Downloads
Documents
netlogon.log - Notepad
File Edit Format View Help

```
Microsoft Windows [Version 10.0.17763.3113]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>Nltest /DBFlag:2080FFFF
SYSTEM\CurrentControlSet\Services\Netlogon\Parameters set to 0x2080ffff
Flags: 0
Connection Status = 0 0x0 NERR_Success
The command completed successfully
```

| Name | Date modified | Type | Size |
|---|---|---|---|
| Dfsr00067.log | 17.07.2022 22:18 | Text Document | 0 KB |
| DfsrApi_001.log | 14.01.2021 21:46 | Text Document | 10 KB |
| mrt.log | 23.06.2022 23:35 | Text Document | 3 KB |
| netlogon.log | 24.07.2022 17:44 | Text Document | 110 KB |

```
07/24 17:43:29 [LOGON] [364] HOMELAB: SamLogon: Network logon of homelab\user3 from MWGMAIN (via MWGMAIN) Entered
07/24 17:43:29 [LOGON] [364] LsaIExtractTargetInfo did not return a Netbios resource server domain name for - no filtering will be done
07/24 17:43:29 [LOGON] [364] HOMELAB: SamLogon: Network logon of homelab\user3 from MWGMAIN (via MWGMAIN) Returns 0xC0000064
07/24 17:43:48 [MISC] [364] HOMELAB: DsGetDcName function called: client PID=6932, Dom:Winserver1.homelab.local Acct:(null) Flags: LDAP
07/24 17:43:48 [MISC] [364] NetpDcInitializeContext: DSGETDC_VALID_FLAGS is c1fffff1
07/24 17:43:48 [MAILSLOT] [364] Received ping from WINSERVER1(Winserver1.homelab.local) Winserver1.homelab.local (null) on <Local>
07/24 17:43:48 [CRITICAL] [364] Ping from WINSERVER1 for domain Winserver1.homelab.local (null) for (null) on <Local> is invalid since
07/24 17:43:48 [CRITICAL] [364] NetpDcGetNameIp: Winserver1.homelab.local: No data returned from DnsQuery.
07/24 17:43:48 [MISC] [364] NetpDcGetName: NetpDcGetNameIp for Winserver1.homelab.local returned 1355
07/24 17:43:48 [CRITICAL] [364] NetpDcGetName: Winserver1.homelab.local: IP and Netbios are both done.
07/24 17:43:48 [MISC] [364] HOMELAB: DsGetDcName function returns 1355 (client PID=6932): Dom:Winserver1.homelab.local Acct:(null) Flag
07/24 17:43:48 [SITE] [364] DsrGetSiteName: Returning site name 'Default-First-Site-Name' from local cache.
07/24 17:43:48 [MISC] [364] HOMELAB: DsGetDcName function called: client PID=6932, Dom:Winserver1.homelab.local Acct:(null) Flags: LDAP
07/24 17:43:48 [MISC] [364] NetpDcInitializeContext: DSGETDC_VALID_FLAGS is c1fffff1
07/24 17:43:48 [MAILSLOT] [364] Received ping from WINSERVER1(Winserver1.homelab.local) Winserver1.homelab.local (null) on <Local>
07/24 17:43:48 [CRITICAL] [364] Ping from WINSERVER1 for domain Winserver1.homelab.local (null) for (null) on <Local> is invalid since
07/24 17:43:48 [MISC] [364] NetpDcGetName: Winserver1.homelab.local similar query failed recently 109
07/24 17:43:48 [MISC] [364] HOMELAB: DsGetDcName function returns 1355 (client PID=6932): Dom:Winserver1.homelab.local Acct:(null) Flag
07/24 17:43:48 [SITE] [364] DsrGetSiteName: Returning site name 'Default-First-Site-Name' from local cache.
07/24 17:44:01 [LOGON] [2280] HOMELAB: SamLogon: Network logon of homelab\user2 from MWGMAIN (via MWGMAIN) Entered
07/24 17:44:01 [LOGON] [2280] LsaIExtractTargetInfo did not return a Netbios resource server domain name for - no filtering will be done
07/24 17:44:01 [LOGON] [2280] HOMELAB: SamLogon: Network logon of homelab\user2 from MWGMAIN (via MWGMAIN) Returns 0xC0000072
07/24 17:44:05 [MISC] [2280] HOMELAB: DsGetDcName function called: client PID=6932, Dom:Winserver1.homelab.local Acct:(null) Flags: LDA
07/24 17:44:05 [MISC] [2280] NetpDcInitializeContext: DSGETDC_VALID_FLAGS is c1fffff1
```

# Secure Web Gateway Troubleshooting – Common Issues

# Secure Web Gateway Troubleshooting – Common Issues
# Disk Space

Disk filled up by:

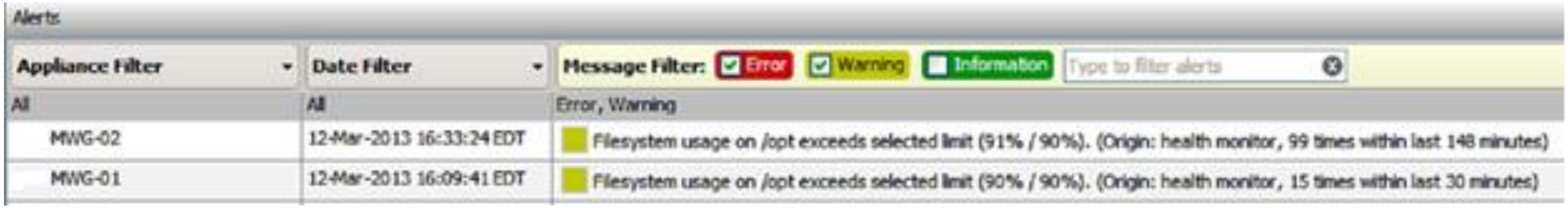
- Log files, debug files (connection/rule traces), core files, temp files, syslog

Results in:

- Login error for GUI
- Not able to save changes (I/O error)
- SWG services not running properly or not started
- User not able to browser

**Dashboard alarms:**

- Filesystem usage on /opt exceeds selected limit
- Filesystem usage on /var exceeds selected limit (/var/log/messages)



| All | All | Error, Warning |
|---|---|---|
| MWG-02 | 12-Mar-2013 16:33:24 EDT | 🟨 Filesystem usage on /opt exceeds selected limit (91% / 90%). (Origin: health monitor, 99 times within last 148 minutes) |
| MWG-01 | 12-Mar-2013 16:09:41 EDT | 🟨 Filesystem usage on /opt exceeds selected limit (90% / 90%). (Origin: health monitor, 15 times within last 30 minutes) |

# Secure Web Gateway Troubleshooting – Common Issues
# Disk Space – cont

- The first thing we have to do with a full disk is to determine where the files are that are filling up the disk. For example is it /var/log or /opt/mwg/log/debug/connection_tracing

- To locate large files (10MB+ here), run:

```
find /opt -type f -size +10000k -exec ls -alsoh {} \;
```

- Once you have determined the location you can see for example /var/log/messages is very large, chances are access logs being logged here. If so rsyslog config is incorrect (very common). Check rsyslog.conf for:

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

  Replace it with this line:

```
*.info;daemon.!=info;mail.none;authpriv.none;cron.none   -/var/log/messages
```

- If connection_tracing directory was connection traces left enabled (very common)

- How to troubleshoot Web Gateway appliance disk space issues:

https://kcm.trellix.com/corporate/index?page=content&id=KB73869

# Secure Web Gateway Troubleshooting – Common Issues – 502 response

- HTTP response code 502 - Bad Gateway

  The server was acting as a gateway or proxy and received an invalid response from the upstream server.

- The three different errors/block pages the client can receive are:

  Host not resolvable

  Bad Response - Web Gateway receives a response from the destination but the response is not a valid HTTP response

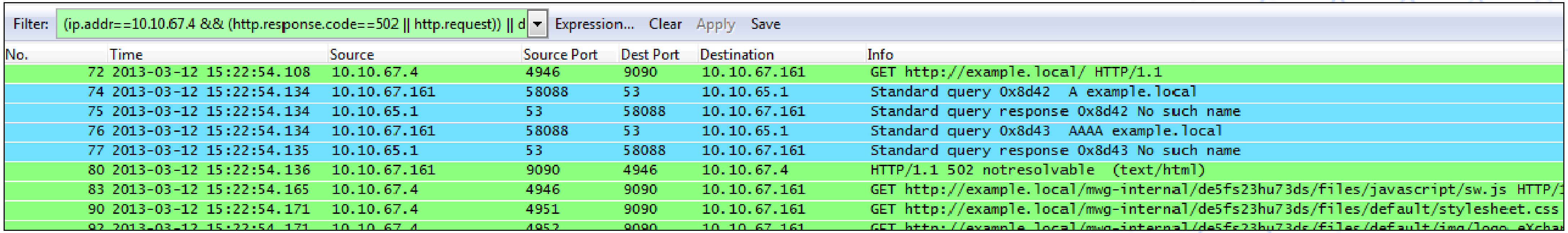
  Cannot Connect

- All three of these blocks will log a HTTP 502 Status in the Web Gateway access logs:

```
[08/Mar/2023:18:25:57 -0600] "" 10.10.67.4 502 "GET
http://example.local/ HTTP/1.1" "" "-" "" 3126 "Mozilla/4.0(compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; .NET
CLR1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR3.5.30729; .NET4.0C; .NET4.0E)" "" "0"
```

# Secure Web Gateway Troubleshooting – Common Issues – 502 response Host not resolvable

- This message will be displayed if Web Gateway is unable to contact the DNS server or if the DNS server returns a “No Such Name” response as seen in the example below. The filter used to display this was “(ip.addr==10.10.67.4 && (http.response.code==502||http.request)) ||dns”.



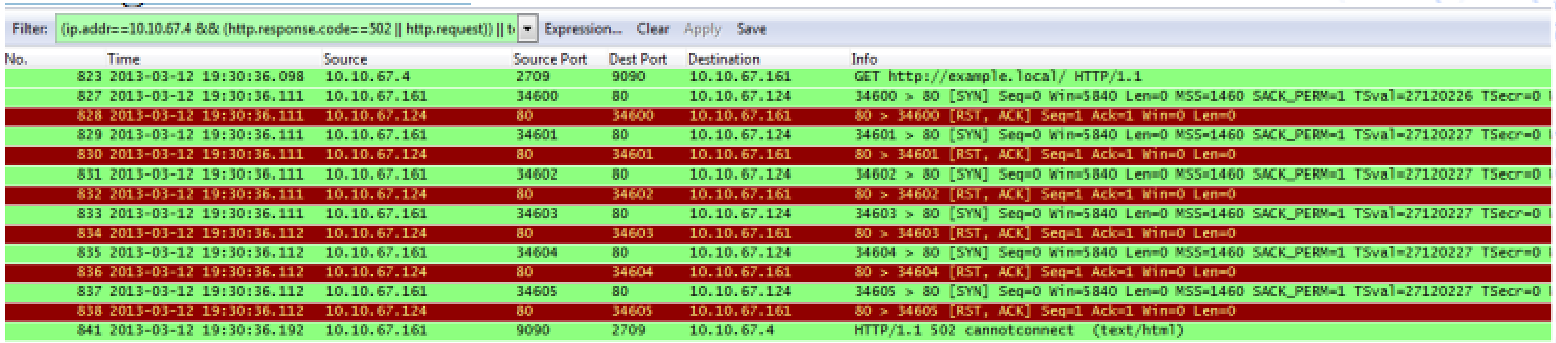
Filter: (ip.addr==10.10.67.4 && (http.response.code==502 || http.request)) || d

| No. | Time | Source | Source Port | Dest Port | Destination | Info |
|---|---|---|---|---|---|---|
| 72 | 2013-03-12 15:22:54.108 | 10.10.67.4 | 4946 | 9090 | 10.10.67.161 | GET http://example.local/ HTTP/1.1 |
| 74 | 2013-03-12 15:22:54.134 | 10.10.67.161 | 58088 | 53 | 10.10.65.1 | Standard query 0x8d42  A example.local |
| 75 | 2013-03-12 15:22:54.134 | 10.10.65.1 | 53 | 58088 | 10.10.67.161 | Standard query response 0x8d42 No such name |
| 76 | 2013-03-12 15:22:54.134 | 10.10.67.161 | 58088 | 53 | 10.10.65.1 | Standard query 0x8d43  AAAA example.local |
| 77 | 2013-03-12 15:22:54.135 | 10.10.65.1 | 53 | 58088 | 10.10.67.161 | Standard query response 0x8d43 No such name |
| 80 | 2013-03-12 15:22:54.136 | 10.10.67.161 | 9090 | 4946 | 10.10.67.4 | HTTP/1.1 502 notresolvable  (text/html) |
| 83 | 2013-03-12 15:22:54.165 | 10.10.67.4 | 4946 | 9090 | 10.10.67.161 | GET http://example.local/mwg-internal/de5fs23hu73ds/files/javascript/sw.js HTTP/1 |
| 90 | 2013-03-12 15:22:54.171 | 10.10.67.4 | 4951 | 9090 | 10.10.67.161 | GET http://example.local/mwg-internal/de5fs23hu73ds/files/default/stylesheet.css |
| 92 | 2013-03-12 15:22:54.171 | 10.10.67.4 | 4952 | 9090 | 10.10.67.161 | GET http://example.local/mwg-internal/de5fs23hu73ds/files/default/img/logo_eXchar |

- In this case we can see the client (10.10.67.4) makes a request to the Web Gateway (10.10.67.161) on its default proxy port 9090. After Web Gateway receives the request it must perform a DNS query to resolve the hostname to an IP address and contacts the DNS server (10.10.65.1), requesting the IP address of example.local. Packets 74 and 76 show the request and packets 75 and 77 show the response.
- To fix this issue the DNS would need to be configured with an “A” record for example.local. A workaround could also be to add it to the Web Gateway’s hosts file. This would allow Web Gateway to resolve the hostname to an IP address without the need of a DNS Query. The hosts file can be edited under **Configuration > File Editor > hosts**.

# Secure Web Gateway Troubleshooting – Common Issues – 502 response Cannot Connect

- Each connection the Web Gateway makes to a destination begins with a **TCP three-way handshake**. This handshake must occur before the Gateway can send the HTTP request and if it fails then it will result in the “Cannot Connect” message. The examples below first shows the initial client request to the Gateway and in the next packet we can see the Gateway sending the first part of the handshake (SYN) to the destination.



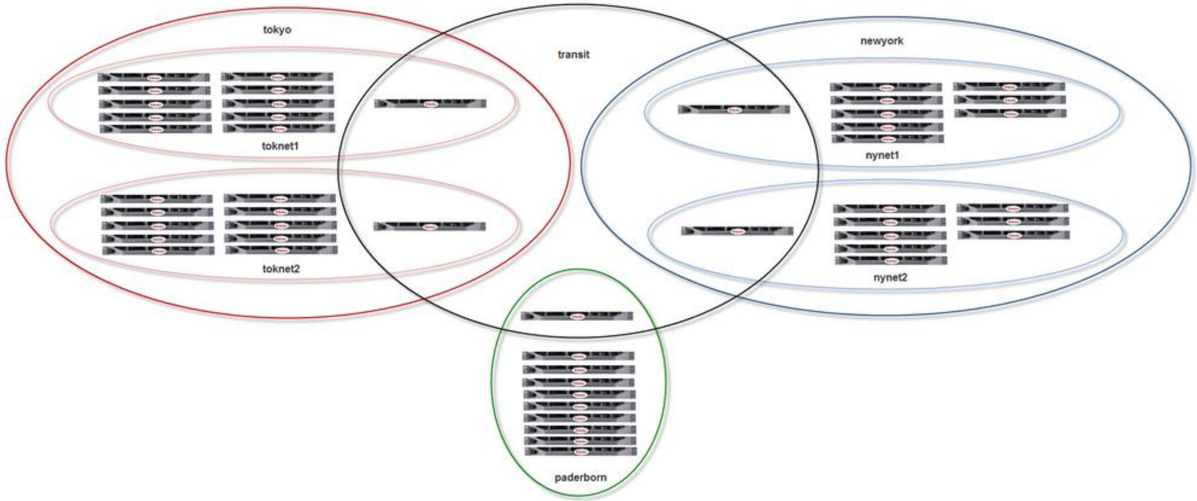
Filter: (ip.addr==10.10.67.4 && (http.response.code==502 || http.request)) || t

| No. | Time | Source | Source Port | Dest Port | Destination | Info |
|---|---|---|---|---|---|---|
| 823 | 2013-03-12 19:30:36.098 | 10.10.67.4 | 2709 | 9090 | 10.10.67.161 | GET http://example.local/ HTTP/1.1 |
| 827 | 2013-03-12 19:30:36.111 | 10.10.67.161 | 34600 | 80 | 10.10.67.124 | 34600 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=27120226 TSecr=0 |
| 828 | 2013-03-12 19:30:36.111 | 10.10.67.124 | 80 | 34600 | 10.10.67.161 | 80 > 34600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 829 | 2013-03-12 19:30:36.111 | 10.10.67.161 | 34601 | 80 | 10.10.67.124 | 34601 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=27120227 TSecr=0 |
| 830 | 2013-03-12 19:30:36.111 | 10.10.67.124 | 80 | 34601 | 10.10.67.161 | 80 > 34601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 831 | 2013-03-12 19:30:36.111 | 10.10.67.161 | 34602 | 80 | 10.10.67.124 | 34602 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=27120227 TSecr=0 |
| 832 | 2013-03-12 19:30:36.111 | 10.10.67.124 | 80 | 34602 | 10.10.67.161 | 80 > 34602 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 833 | 2013-03-12 19:30:36.111 | 10.10.67.161 | 34603 | 80 | 10.10.67.124 | 34603 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=27120227 TSecr=0 |
| 834 | 2013-03-12 19:30:36.112 | 10.10.67.124 | 80 | 34603 | 10.10.67.161 | 80 > 34603 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 835 | 2013-03-12 19:30:36.112 | 10.10.67.161 | 34604 | 80 | 10.10.67.124 | 34604 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=27120227 TSecr=0 |
| 836 | 2013-03-12 19:30:36.112 | 10.10.67.124 | 80 | 34604 | 10.10.67.161 | 80 > 34604 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 837 | 2013-03-12 19:30:36.112 | 10.10.67.161 | 34605 | 80 | 10.10.67.124 | 34605 > 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=27120227 TSecr=0 |
| 838 | 2013-03-12 19:30:36.112 | 10.10.67.124 | 80 | 34605 | 10.10.67.161 | 80 > 34605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 841 | 2013-03-12 19:30:36.192 | 10.10.67.161 | 9090 | 2709 | 10.10.67.4 | HTTP/1.1 502 cannotconnect (text/html) |

- After the initial client connection sent in packet 823, Web Gateway tries to establish a connection to the destination by sending a SYN packet. Normally we would expect to see a SYN/ACK packet sent back from the server but in this case packets 828, 830, 832, etc… all show that the Web Gateway is receiving a RST (Reset) packet after each SYN packet it sends. The RST packet is used to terminate a connection.  Since Web Gateway is unable to establish a TCP connection to the destination a “Cannot Connect” message is sent back to the client. It might also happen that there is no answer to the SYN at all. In any case, you need to inspect the upstream devices.

# Secure Web Gateway Troubleshooting – Common Issues
# Cluster

As a best practice, we recommend only putting up to 10 nodes behind a single transit node. If you have more than 10 nodes in a location, you should have more than one transit node and create smaller network groups that are tied to the transit node. Here's an example with a larger cluster with nodes in Tokyo, New York, and Paderborn. For the smaller locations with one transit node, the Runtime and network groups use the same name.

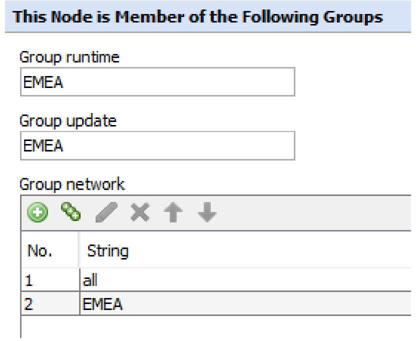


# Secure Web Gateway Troubleshooting – Common Issues Cluster

## Management IP, Time Sync, Groups, Timeout values

Results in:

- Sync issue
- Login failure
- Fail to save change



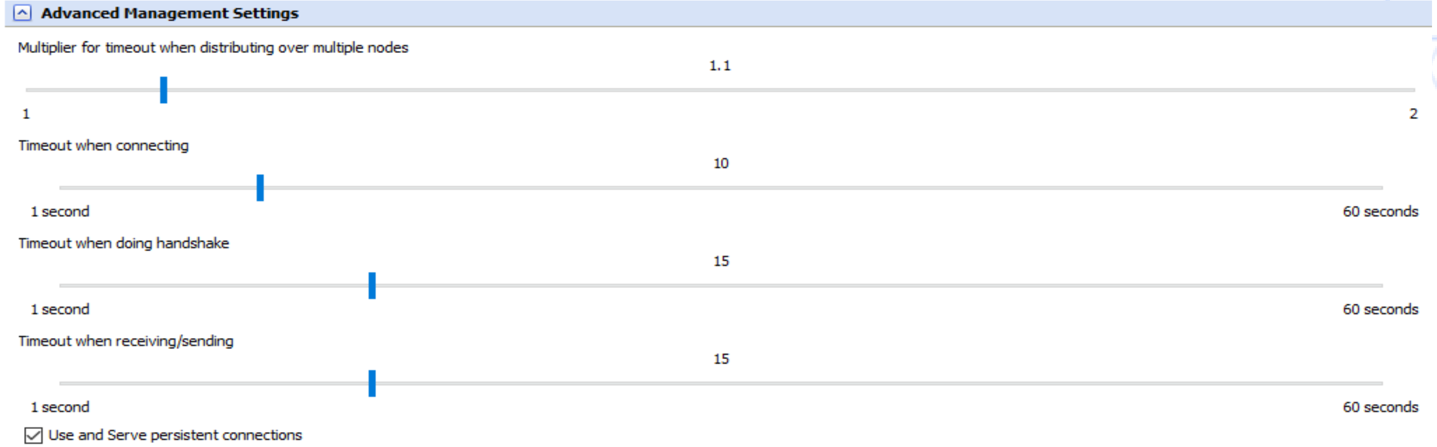
This Node is Member of the Following Groups

Group runtime: EMEA

Group update: EMEA

Group network

| No. | String |
|---|---|
| 1 | all |
| 2 | EMEA |



Advanced Management Settings

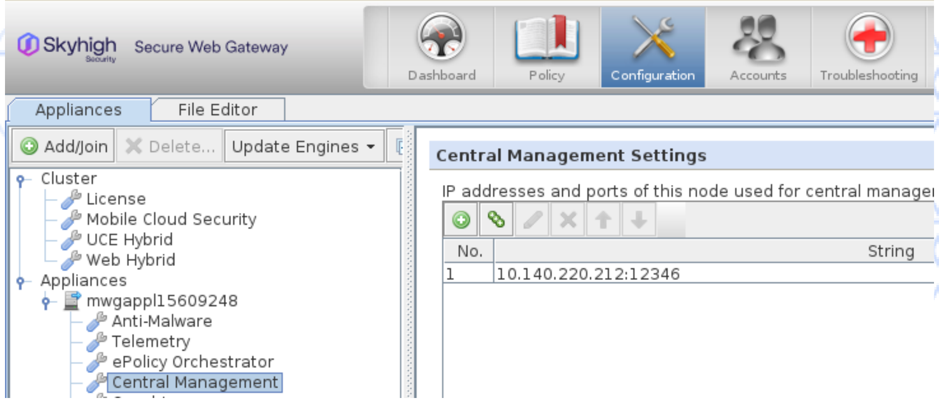
Multiplier for timeout when distributing over multiple nodes: 1.1 (1 – 2)

Timeout when connecting: 10 (1 second – 60 seconds)

Timeout when doing handshake: 15 (1 second – 60 seconds)

Timeout when receiving/sending: 15 (1 second – 60 seconds)

☑ Use and Serve persistent connections

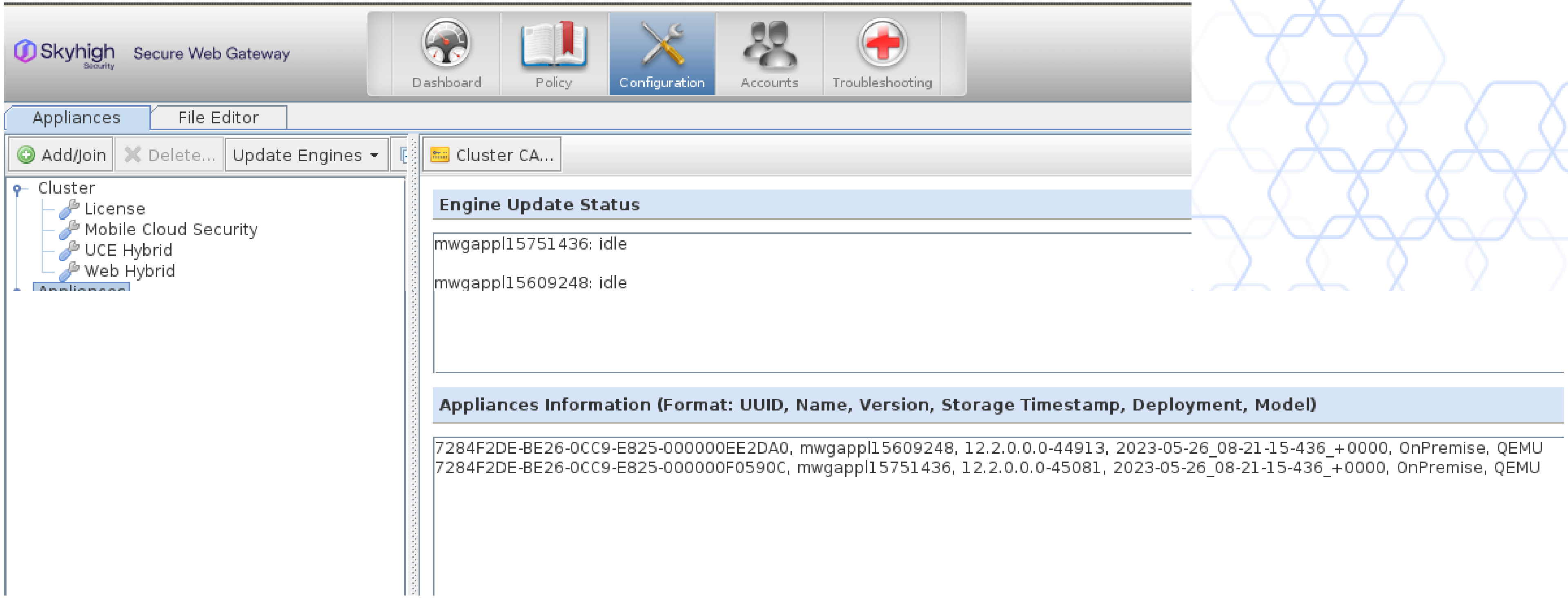


Central Management Settings

IP addresses and ports of this node used for central managei

| No. | String |
|---|---|
| 1 | 10.140.220.212:12346 |

# Secure Web Gateway Troubleshooting – Common Issues Cluster - cont



Engine Update Status

```
mwgappl15751436: idle

mwgappl15609248: idle
```

Appliances Information (Format: UUID, Name, Version, Storage Timestamp, Deployment, Model)

```
7284F2DE-BE26-0CC9-E825-000000EE2DA0, mwgappl15609248, 12.2.0.0.0-44913, 2023-05-26_08-21-15-436_+0000, OnPremise, QEMU
7284F2DE-BE26-0CC9-E825-000000F0590C, mwgappl15751436, 12.2.0.0.0-45081, 2023-05-26_08-21-15-436_+0000, OnPremise, QEMU
```

# The perfect Service Request

- Detailed description / date & time of issue; expectation vs. given behaviour
- Feedback file
- Tcpdump on Client + SWG (filtered if needed) Client IP and requested URL
- Connection Traces
- Rule Trace
- Details on infrastructure (complex setup)
- Steps already performed as troubleshooting

Skyhigh Security

# Thank You!

www.skyhighsecurity.com

Skyhigh
Security

# Q and A

www.skyhighsecurity.com