

# SWG troubleshooting and common scenarios



## Overview

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

# Software & License

- SWG Software & License  
<https://contentsecurity.skyhigh.cloud>
- Skyhigh Client Proxy (SCP), CSR & others  
<https://www.trellix.com/en-us/downloads.html>
- License issues SWG:  
Contact [licensing@trellix.com](mailto:licensing@trellix.com)
- SWG FAQs:  
<https://kcm.trellix.com/corporate/index?page=content&id=KB77816>

Download the Web Gateway Appliance ISO images.

### Important Announcement

Skyhigh Security performed a clean-up of the SWG download portal, Content & Cloud Security Portal.

The following versions have been removed from the portal, effective January 27, 2021.

- 7.6.x and older
- 7.7.x
- 7.8.1

After January 27, 2021, there is no way of downloading the older builds. Please contact support if you have any questions.

### 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
- 8.0.0 and higher

### Skyhigh Secure Web Gateway Main Release

Product	Version	Build	Filesize	Release Date	Release Notes	Filetype
McAfee Web Gateway Appliance ISO	10.2.11	41081	717 MB	Jun 14, 2022		.iso
McAfee Web Gateway Appliance USB	10.2.11	41081	846 MB	Jun 14, 2022		.usb
Open Source Components <a href="#">↗</a>			-	-	-	-

### Skyhigh Secure Web Gateway Controlled Release

Product	Version	Build	Filesize	Release Date	Release Notes	Filetype
McAfee Web Gateway Appliance ISO	11.2.0	41149	756 MB	Jun 21, 2022		.iso
McAfee Web Gateway Appliance USB	11.2.0	41149	897 MB	Jun 21, 2022		.usb
Open Source Components <a href="#">↗</a>			-	-	-	-

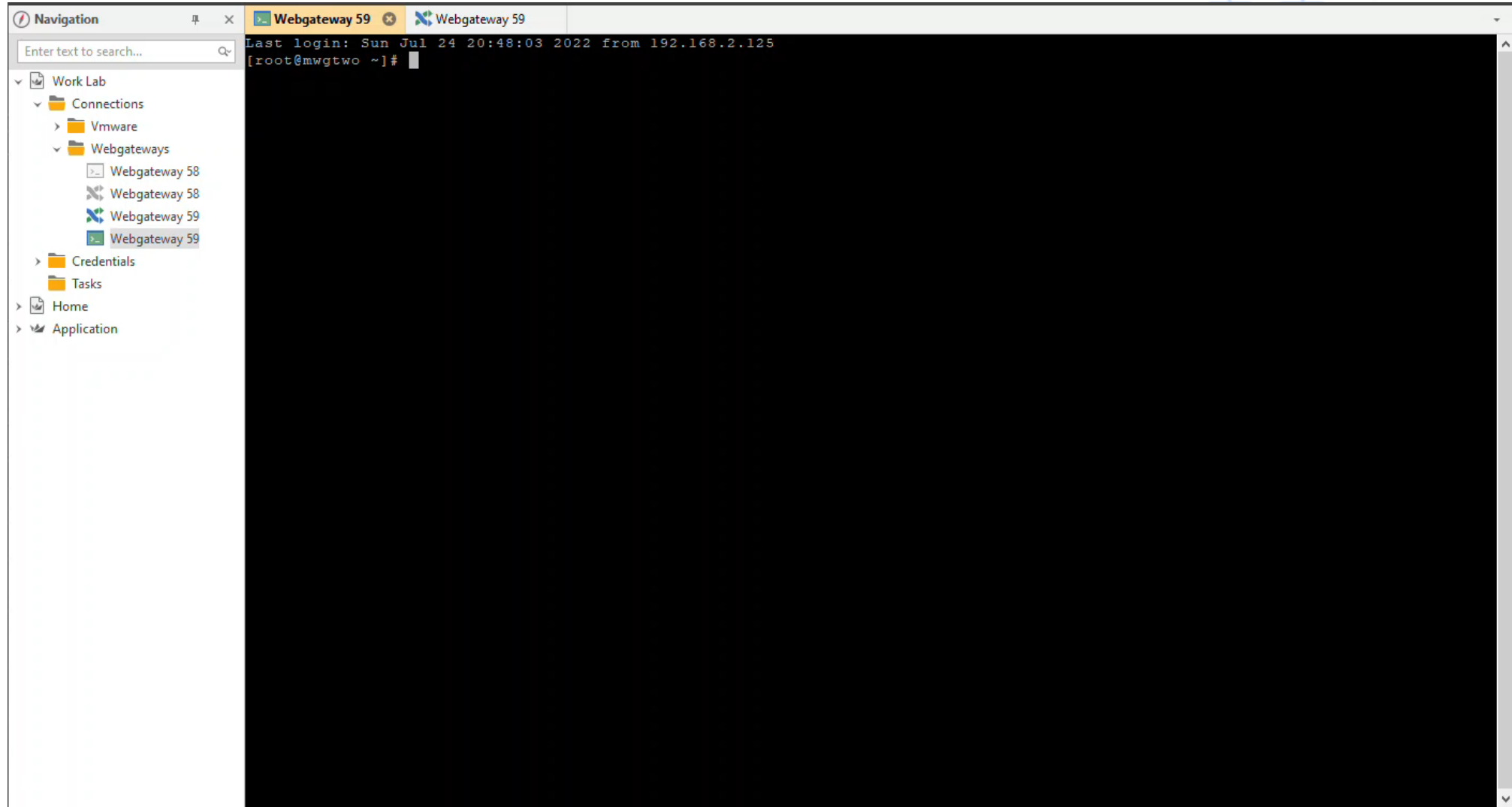
#### Downloads

- > Software
- > Beta
- > ICAP Clients
- > Tools
- > Archive
- > Language Packs
- > BIOS
- > Internal Archive

# 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>
- Getlogs script (hardware log)
- Required information
- For all hardware topics such as:
  - RAID reports 1 critical disks and 1 failing disks
  - BBU - Battery replacement required
  - MWG not starting

# Hardware Troubleshooting - cont



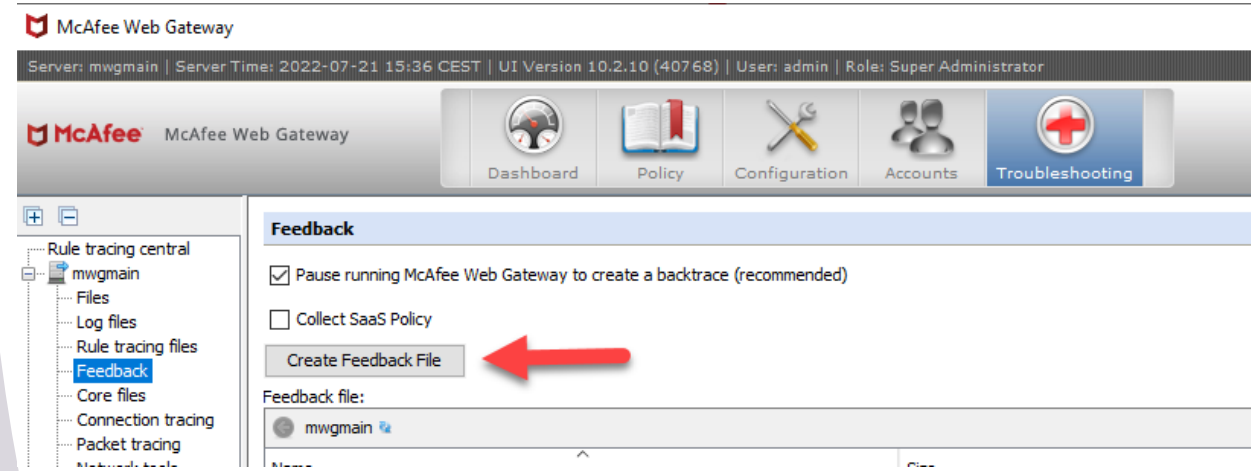
# Secure Web Gateway Troubleshooting

- Feedback file
- Rule traces (identify delays, flow through policy)
- 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://kcm.trellix.com/corporate/index?page=content&id=KB63289>

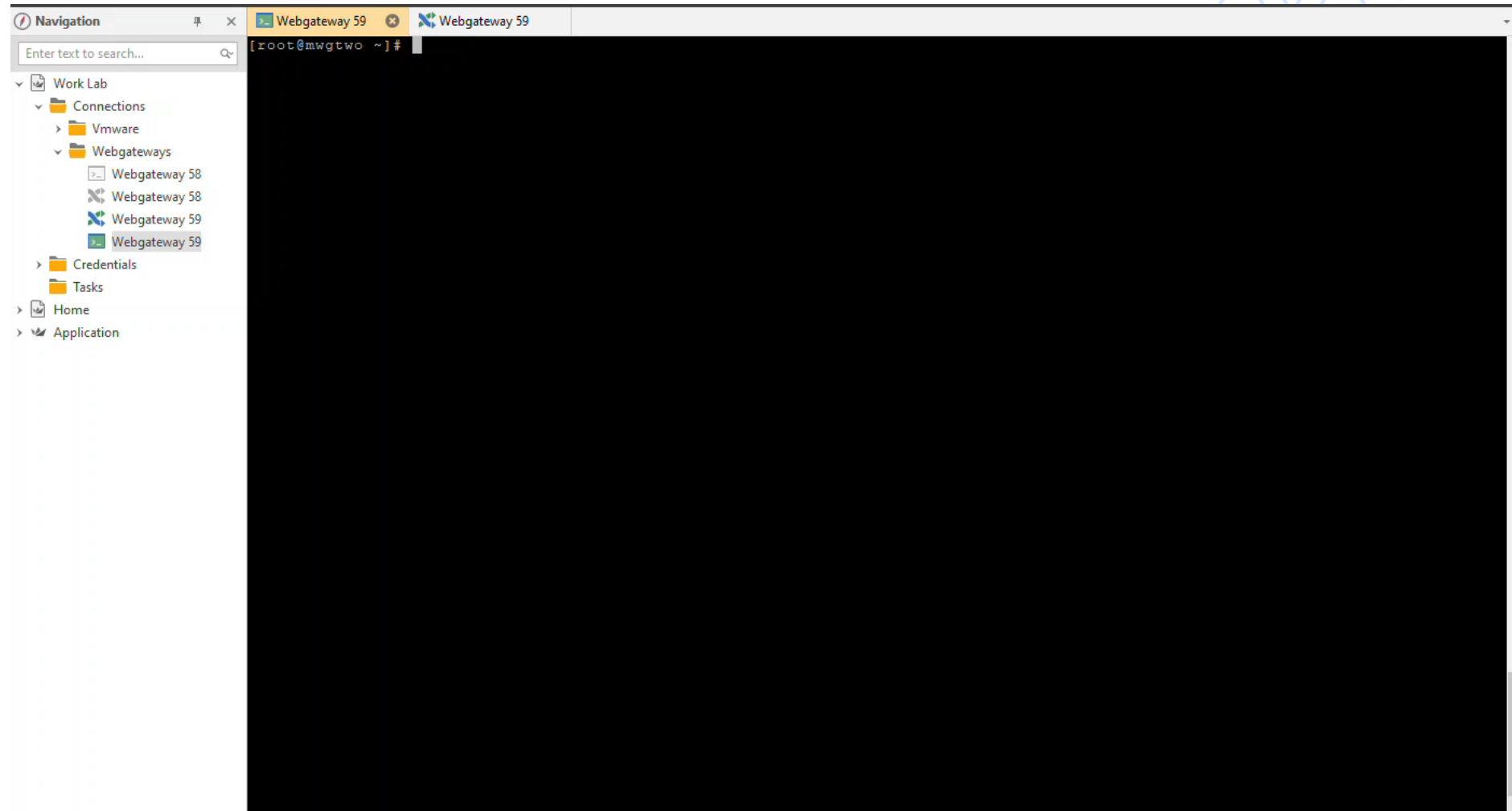


The screenshot displays the McAfee Web Gateway administration interface. At the top, the title bar reads "McAfee Web Gateway" and the status bar shows "Server: mwgmain | Server Time: 2022-07-21 15:36 CEST | UI Version 10.2.10 (40768) | User: admin | Role: Super Administrator". Below this is a navigation menu with icons for Dashboard, Policy, Configuration, Accounts, and Troubleshooting. The left sidebar contains a tree view with "Feedback" selected under "Rule tracing files". The main content area is titled "Feedback" and includes the following options:

- Pause running McAfee Web Gateway to create a backtrace (recommended)
- Collect SaaS Policy
- Create Feedback File** (highlighted with a red arrow)

Below these options, the "Feedback file:" section shows a dropdown menu with "mwgmain" selected.

# Secure Web Gateway Troubleshooting - Feedback File - Cont





# Secure Web Gateway Troubleshooting - Rule Traces

- Troubleshooting > Rule Tracing Central

The screenshot shows the McAfee Web Gateway interface. The top navigation bar includes Dashboard, Policy, Configuration, Accounts, and Troubleshooting. The main area is titled "Rule tracing central" and shows a search for "https://www.youtube.com" with a "Go" button. The results table shows a single entry at 16:11:45 with the URL "https://www.youtube.com". The right-hand pane displays the rule configuration for "https://www.youtube.com", including a list of actions such as "Allow URLs That Match in URL Whitelist for Default Groups" and "Enable SafeSearchEnforcer". The "Top Properties" section shows details like URL, Client IP, User-Agent, and Block.Reason (CONNECT).

The screenshot shows the McAfee Web Gateway interface. The top navigation bar includes Dashboard, Policy, Configuration, Accounts, and Troubleshooting. The main area is titled "Rule tracing central" and shows a search for "https://www.youtube.com/" with a "Go" button. The results table shows a single entry at 16:18:15 with the URL "https://www.youtube.com/" and a red "Blocked" icon. The right-hand pane displays the rule configuration for "https://www.youtube.com/", including a list of actions such as "Initialize Policy Filtered Flag" and "Block URLs Whose Category Is in Category Blocklist for Default Groups". The "Top Properties" section shows details like Cycle: Request - 327µs (Block URLs Whose Category Is in Category Blocklist for Default Groups). The "Criteria" section shows a rule that is evaluated as "not included in trace" and the "Action" is "Block <URL Blocked>".

# Secure Web Gateway Troubleshooting - Rule Traces - Cont

The screenshot shows the McAfee Web Gateway administration console. The top navigation bar includes 'Dashboard', 'Policy', 'Configuration', 'Accounts', and 'Troubleshooting'. The 'Rule tracing central' section is active, showing a search filter for 'mwigmain' and '192.168.2.125'. Below the search bar, there are options for 'Filter by' (Source) and 'Export'. A table with columns 'Time' and 'URL' is visible, but it is currently empty. The left sidebar shows a tree view of the system's configuration and logs.

The screenshot shows the Google homepage in a browser window. The address bar displays 'https://www.google.com'. The page features the Google logo, a search bar, and buttons for 'Google Suche' and 'Auf gut Glück!'. The footer includes links for 'Deutschland', 'CO<sub>2</sub>-neutral seit 2007', 'Werbeprogramme', 'Unternehmen', 'Wie funktioniert die Google Suche?', 'Datenschutzerklärung', 'Nutzungsbedingungen', and 'Einstellungen'.

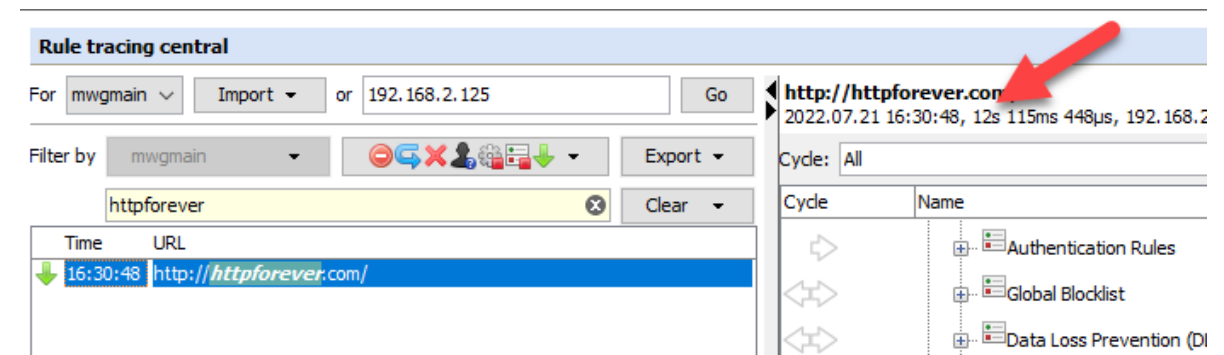
# Secure Web Gateway Troubleshooting - GTI delays

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

Failure to allow access to our 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=KB79640>

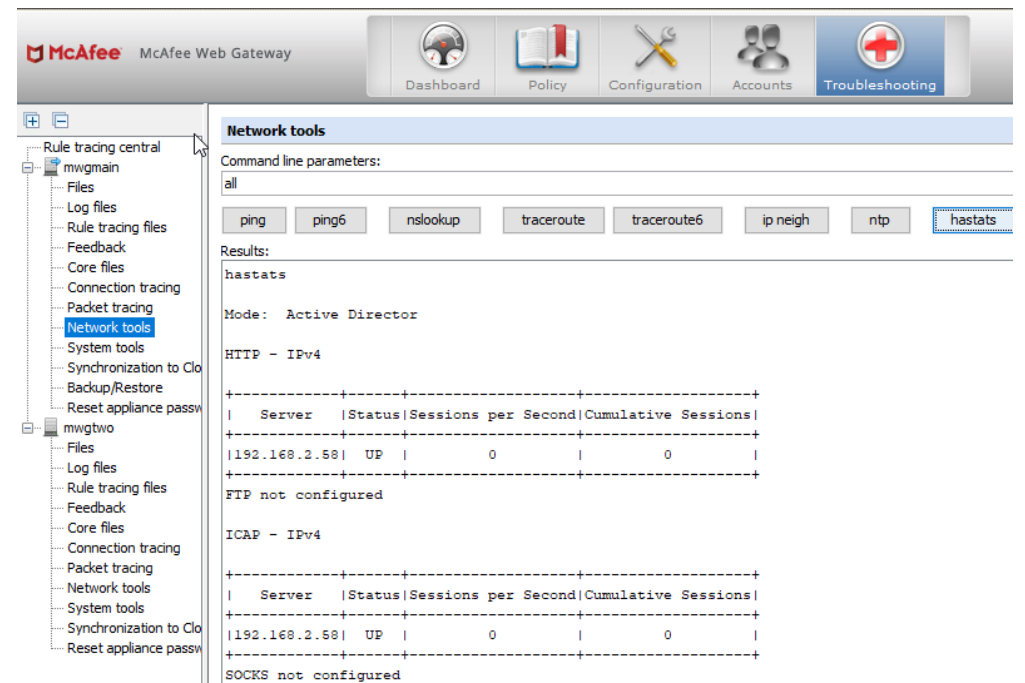


The screenshot displays the 'Rule tracing central' interface. At the top, there is a search bar with 'mwgmain' selected in the 'For' dropdown, 'Import' in the 'Import' dropdown, and '192.168.2.125' in the search field. A 'Go' button is to the right. Below this, the 'Filter by' section shows 'mwgmain' in a dropdown, followed by several icons (a red minus sign, a blue refresh, a red X, a person icon, a globe, and a green down arrow) and an 'Export' dropdown. A search box contains 'httpforever' with a 'Clear' button. Below the search box is a table with two columns: 'Time' and 'URL'. The first row shows a green down arrow in the 'Time' column and '16:30:48' in the 'URL' column, with the URL 'http://httpforever.com/' highlighted in blue. To the right of the table is a sidebar with a tree view. The root node is 'http://httpforever.com' with a red arrow pointing to it. Below it are three sub-nodes: 'Authentication Rules', 'Global Blocklist', and 'Data Loss Prevention (DI)'. The 'Cycle' dropdown is set to 'All'.

# 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.

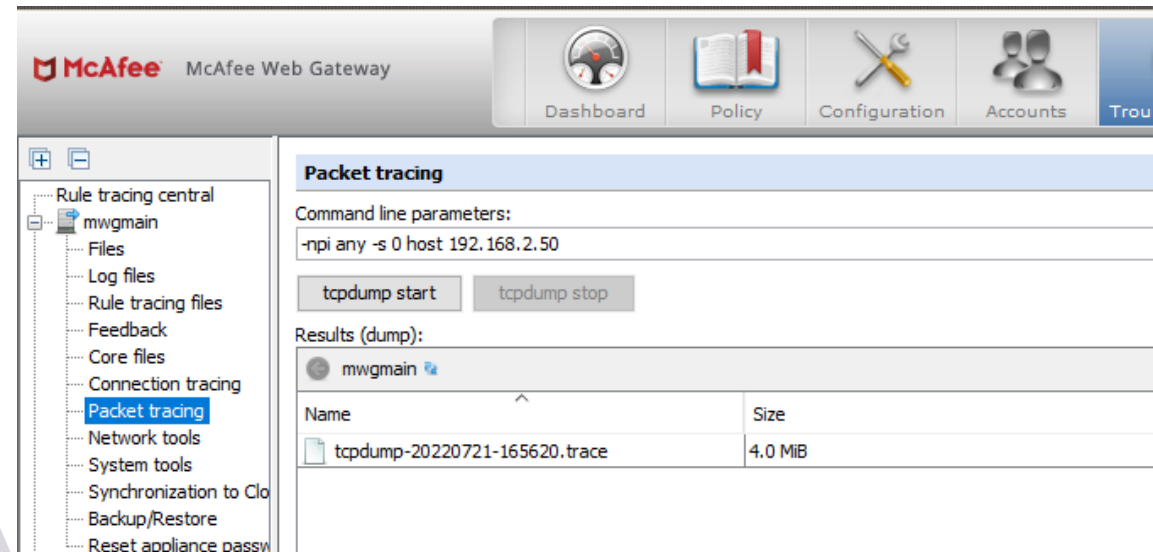


The screenshot shows the McAfee Web Gateway interface with the 'Network tools' section selected in the left-hand navigation pane. The main content area displays the 'Network tools' configuration page. Under 'Command line parameters', the value 'all' is entered. Below this, there are buttons for various tools: ping, ping6, nslookup, traceroute, traceroute6, ip neigh, ntp, and hastats. The 'Results' section shows the output of the 'hastats' command, indicating that the system is in 'Active Director' mode and that HTTP, ICAP, and SOCKS services are configured for IPv4. Two tables show the status of these services, both indicating 'UP' status with 0 sessions per second and 0 cumulative sessions.

Server	Status	Sessions per Second	Cumulative Sessions
192.168.2.58	UP	0	0

Server	Status	Sessions per Second	Cumulative Sessions
192.168.2.58	UP	0	0



The screenshot shows the McAfee Web Gateway interface with the 'Packet tracing' section selected in the left-hand navigation pane. The main content area displays the 'Packet tracing' configuration page. Under 'Command line parameters', the value '-npi any -s 0 host 192.168.2.50' is entered. Below this, there are buttons for 'tcpdump start' and 'tcpdump stop'. The 'Results (dump)' section shows a table with one entry: a file named 'tcpdump-20220721-165620.trace' with a size of 4.0 MiB.

Name	Size
tcpdump-20220721-165620.trace	4.0 MiB

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

## Troubleshooting > Packet Tracing | Network Tools

- -s 0 (snap length - amount of data for each frame; 0 no limit)
- -npi any (don't convert host/ports, no promiscuous mode, all interfaces)
- host www.mcafee.com or host 10.11.12.13
- port 445
  
- 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 &`
  
- -Z user
- -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

The screenshot displays the McAfee Web Gateway administration console. The top navigation bar includes 'Dashboard', 'Policy', 'Configuration', 'Accounts', and 'Troubleshooting' (which is active). The 'Network tools' section is open, showing a 'Command line parameters:' input field and a row of tool buttons: 'ping', 'ping6', 'nsllookup', 'tracertoute', 'tracertoute6', 'ip neigh', 'ntp', and 'hastats'. The 'Results:' area below shows the text 'Cancelled!'. A left-hand sidebar contains a tree view of system components, with 'Network tools' highlighted under the 'mwtwo' instance. The top status bar shows 'Server: mwgmain | Server Time: 2022-07-24 23:48 CEST | UI Version 10.2.10 (40768) | User: admin | Role: Super Administrator'.



# 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

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	8.690484	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	TCP	443.49246 [ACK] Seq=1030802300 Ack=36027218
1835	10.201531	216.239.98.121	192.168.1.101	TCP	443.49246 [ACK] Seq=36027218 Ack=1030802301 W
1836	11.798841	192.168.1.101	111.221.29.129	SSL	Continuation Data
1837	12.045607	111.221.29.129	192.168.1.101	TCP	443.65343 [ACK] Seq=41277483 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=41277616 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

```
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  .....pagead2.g
0040  6f 6f 67 6c 65 73 79 6e 64 89 63 61 74 69 6f 6e  eoglesyn dication
0050  03 63 6f 6d 00 00 01 00 01  .....com.....
```

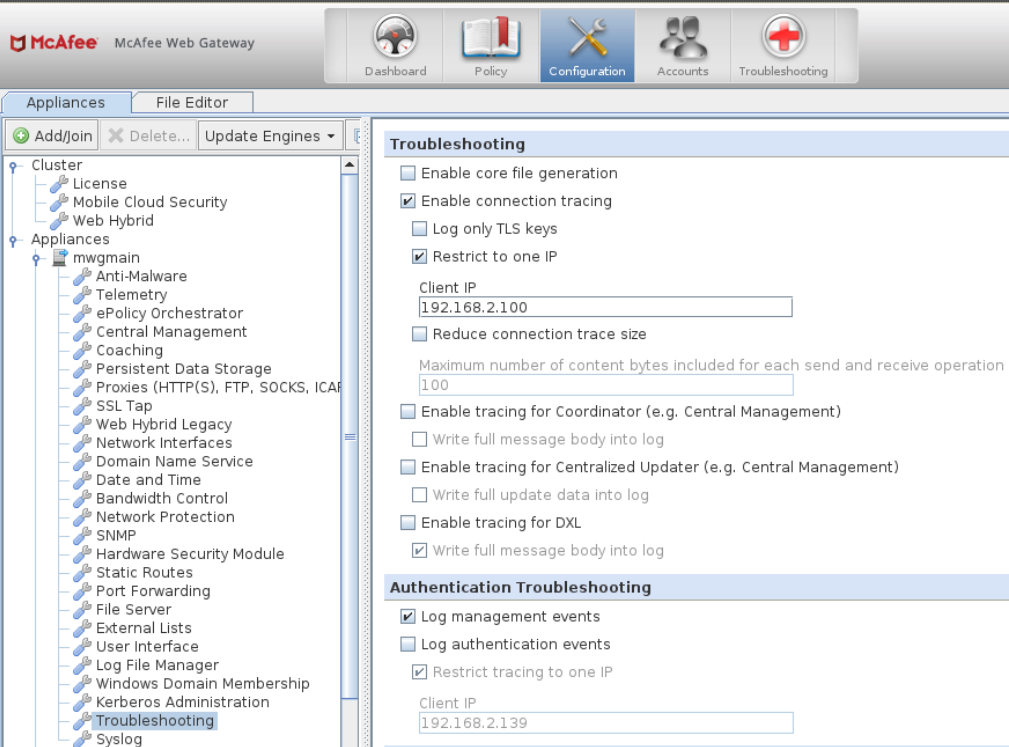
# Secure Web Gateway Troubleshooting – Connection Traces

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:** Only possible if SSL Scanning is enabled



The screenshot displays the McAfee Web Gateway configuration interface. The top navigation bar includes icons for Dashboard, Policy, Configuration, Accounts, and Troubleshooting. The main content area is divided into a left-hand tree view and a right-hand configuration panel.

**Left Panel (Tree View):**

- Cluster
  - License
  - Mobile Cloud Security
  - Web Hybrid
- Appliances
  - mwgmain
    - Anti-Malware
    - Telemetry
    - ePolicy Orchestrator
    - Central Management
    - Coaching
    - Persistent Data Storage
    - Proxies (HTTP(S), FTP, SOCKS, ICA)
    - SSL Tap
    - Web Hybrid Legacy
    - Network Interfaces
    - Domain Name Service
    - Date and Time
    - Bandwidth Control
    - Network Protection
    - SNMP
    - Hardware Security Module
    - Static Routes
    - Port Forwarding
    - File Server
    - External Lists
    - User Interface
    - Log File Manager
    - Windows Domain Membership
    - Kerberos Administration
    - Troubleshooting**
    - Syslog

**Right Panel (Configuration):**

**Troubleshooting**

- Enable core file generation
- Enable connection tracing
  - Log only TLS keys
  - Restrict to one IP
    - Client IP:
  - Reduce connection trace size
    - Maximum number of content bytes included for each send and receive operation:
- 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 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

The screenshot displays the McAfee Web Gateway management console. The left sidebar shows a tree view of configuration options, with 'Troubleshooting' and 'Syslog' selected. The main area is divided into 'Troubleshooting' and 'Connection tracing' sections. The 'Connection tracing' section shows a list of trace files for the 'mwgapplaw' appliance, including 'HTTP-100490-C.txt' through 'HTTP-100493-S.txt'. Two log windows are open, showing detailed connection traces for 'HTTP-100495-C.txt' and 'HTTP-100495-S.txt'. The logs show the sequence of events from connection establishment to the final response, including headers, status codes, and connection state changes.

```
1 18:13:39.949: Accepted connection on 172.27.96.188:9090 from 10.140.132.50:62200 (fd = 86, data
2 18:13:39.949: Received 215 bytes
3 >>>
4 CONNECT mcafee.com:443 HTTP/1.0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
6 Host: mcafee.com:443
7 Content-Length: 0
8 DNT: 1
9 Proxy-Connection: Keep-Alive
10 Pragma: no-cache
11 <<<<
12 18:13:39.950: Send 39 bytes; offset = 0
13 >>>
14 HTTP/1.0 200 Connection established
15 <<<<
16 18:13:40.084: Peaked 199 bytes
17 >>>
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 mcafee.com[REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 <<<<
29 18:13:40.599: SSL Accept: Would Block: (EPOLLIN, EPOLLONESHOT)
30 18:13:40.608: SSL Accept finished ok. Session re-use = 0, cipher = ECDHE-RSA-AES256-GCM-SHA384
31 18:13:40.608: New logical connection SocketOptions unchanged. TCP window not empty: 242 bytes (or 1
32 18:13:40.608: Receive: Would Block (EPOLLIN, EPOLLONESHOT)
33 18:13:40.609: Received 274 bytes
34 [[[[
35 GET / HTTP/1.1
36 Accept: text/html, application/xhtml+xml, image/jxr, */*
37 Accept-Language: de-DE,de;q=0.5
38 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
39 Accept-Encoding: gzip, deflate
40 Host: mcafee.com
41 DNT: 1
42 Connection: Keep-Alive
43 [[[[
44 18:13:40.750: Connection is still ok
45 18:13:40.823: Send 279 bytes; offset = 0
46 [[[[
47 HTTP/1.1 301 Moved Permanently
48 Via: 1.1 172.27.96.188 (McAfee Web Gateway 7.7.2.8.0.25114)
49 Date: Mon, 12 Feb 2018 18:13:40 GMT
```

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

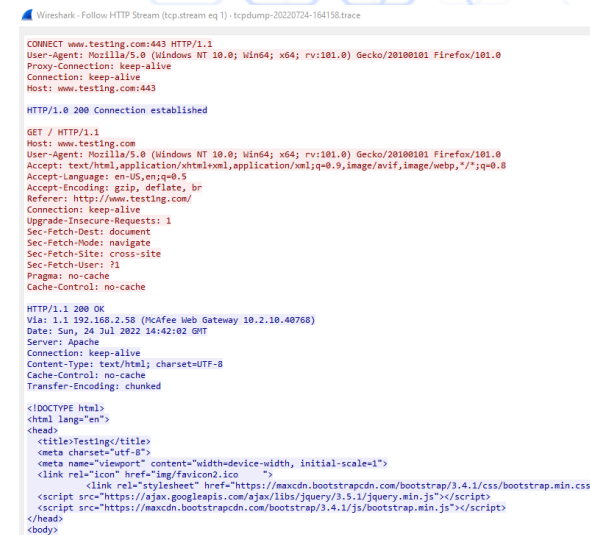
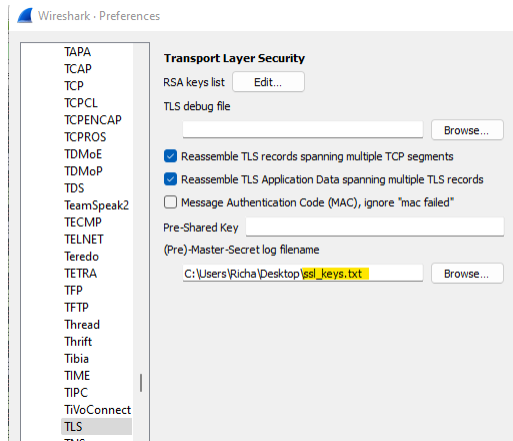
Take aways:

- 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, 0x00, 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 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:



# Secure Web Gateway Troubleshooting – Core Dump

High CPU.

High Memory / Memory Leak.

Crashes / Services / Server

The screenshot shows the McAfee Web Gateway administration interface. The top navigation bar includes 'Dashboard', 'Policy', 'Configuration', 'Accounts', and 'Troubleshooting'. The 'Configuration' tab is active, and the 'Troubleshooting' sub-tab is selected. The left sidebar shows a tree view of the system components, with 'Troubleshooting' selected under the 'mwgmain' appliance. The main content area displays the 'Troubleshooting' configuration options:

- Enable core file generation
- Enable connection tracing
  - Log only TLS keys
  - Restrict to one IP
    - Client IP: 192.168.2.149
  - 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 DXL
  - Write full message body into log

**Authentication Troubleshooting**

- Log management events
- Log authentication events
  - Restrict tracing to one IP
    - Client IP: 192.168.2.149

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

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

```
# The format should be something like:
```

```
# mv <nameofcreatedcorefile> mwg-core-3902.core
```

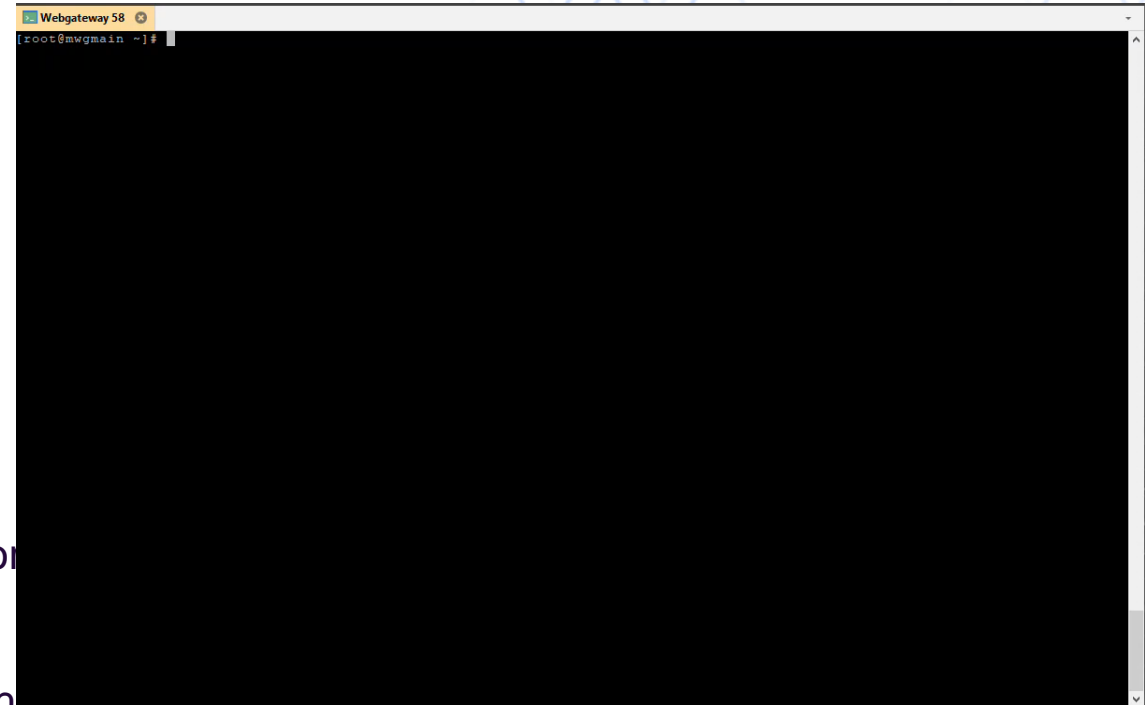
Compress the core file (we use 'gzip -9' in case it is larger than 4GB), substitute '[FILENAME]' with the filename of the desired core file:

```
# 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

The screenshot displays the McAfee Web Gateway Configuration console. The left-hand navigation pane shows a tree structure with 'Appliances' expanded to 'mwgmain', and 'Troubleshooting' selected. The right-hand pane shows the configuration for 'Troubleshooting' and 'Authentication Troubleshooting'. The 'Authentication Troubleshooting' section is highlighted in yellow.

**McAfee Web Gateway**

Dashboard Policy Configuration Accounts Troubleshooting

Appliances File Editor

Add/Join Delete... Update Engines

Cluster

- License
- Mobile Cloud Security
- Web Hybrid

Appliances

- mwgmain
  - Anti-Malware
  - Telemetry
  - ePolicy Orchestrator
  - Central Management
  - Coaching
  - Persistent Data Storage
  - Proxies (HTTP(S), FTP, SOCKS, ICA)
  - SSL Tap
  - Web Hybrid Legacy
  - Network Interfaces
  - Domain Name Service
  - Date and Time
  - Bandwidth Control
  - Network Protection
  - SNMP
  - Hardware Security Module
  - Static Routes
  - Port Forwarding
  - File Server
  - External Lists
  - User Interface
  - Log File Manager
  - Windows Domain Membership
  - Kerberos Administration
  - Troubleshooting**
  - Syslog

**Troubleshooting**

- Enable core file generation
- Enable connection tracing
- Log only TLS keys
- Restrict to one IP
  - Client IP: 192.168.2.149
- Reduce connection trace size
- Maximum number of content bytes included for each send and receive: 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 DXL
  - Write full message body into log

**Authentication Troubleshooting**

- Log management events
- Log authentication events
- Restrict tracing to one IP
  - Client IP: 192.168.2.149

# 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 17:20:26.768 +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/de5f23hu73ds/plugin?
target-Auth&reason-Auth&ClientID=1752291987&tl=600&url=ahR&DovL3RlC3QxbmcuY29tLw,,&nd=1658675433.155593410.d1klvarI6v8ck5jXWAtP8Kp713eHII9UtoV_otlEfs,
[2022-07-24 17:20:46.177 +02:00] [398] NTLM (127, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff804599c0 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 17:20:46.182 +02:00] [398] NTLM (127, 192.168.2.149) URL: http://192.168.2.58:9090/mwg-internal/de5f23hu73ds/plugin?
target-Auth&reason-Auth&ClientID=1752291987&tl=600&url=ahR&DovL3RlC3QxbmcuY29tLw,,&nd=1658675433.155593410.d1klvarI6v8ck5jXWAtP8Kp713eHII9UtoV_otlEfs,
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff804599c0 RR: 0x555e944aa690
[2022-07-24 17:20:46.182 +02:00] [398] NTLM (128, 192.168.2.149) Incoming credentials: NTLM TlRMTWNTUAABAAAABIIogAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAKPBVAAAADw=
[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 TlRMTWNTUAACAAAAAAAAAAAAAAAAAFgong02DjVzr952AAAAAAAAAAAAAAAAAAAA
[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/de5f23hu73ds/plugin?
target-Auth&reason-Auth&ClientID=1752291987&tl=600&url=ahR&DovL3RlC3QxbmcuY29tLw,,&nd=1658675433.155593410.d1klvarI6v8ck5jXWAtP8Kp713eHII9UtoV_otlEfs,
[2022-07-24 17:20:46.186 +02:00] [398] NTLM (129, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff804599c0 RR: 0x555e944a1f80
[2022-07-24 17:20:46.186 +02:00] [398] NTLM (129, 192.168.2.149) Incoming credentials: NTLM
TlRMTWNTUADAAAGAAAYAT4AACSAkwp9AAAAADgBYAAACgAKAGYAAAAAB9A4AAAAAABSAQA0ABYklogoA8FUAAAAP/ittFvopHqjlgzjXDV2gAbwTAAAGIABHAGIAd0BzAGUAcgYAEQAR0BTAESAAVAPFA
ERT2may2Y6HwBAQAAAAAAAD0EM115n9g8y8Tz7p4e2YAAAAACAAwAAAAAABAAAAAAGAACM3dSmD0hRvW473/DCICgkE/tAkRPUlqZwE5YKCoEAAAAAAAAAAAAAAAAAAAAAAAEgAVABUAFALwAA
[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/de5f23hu73ds/plugin?
target-Auth&reason-Auth&ClientID=1752291987&tl=600&url=ahR&DovL3RlC3QxbmcuY29tLw,,&nd=1658675433.155593410.d1klvarI6v8ck5jXWAtP8Kp713eHII9UtoV_otlEfs,
[2022-07-24 17:21:32.522 +02:00] [433] NTLM (130, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff804599c0 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: 0, 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/de5f23hu73ds/plugin?
target-Auth&reason-Auth&ClientID=1752291987&tl=600&url=ahR&DovL3RlC3QxbmcuY29tLw,,&nd=1658675433.155593410.d1klvarI6v8ck5jXWAtP8Kp713eHII9UtoV_otlEfs,
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff804599c0 RR: 0x7ff87c0223f0
[2022-07-24 17:21:32.526 +02:00] [433] NTLM (131, 192.168.2.149) Incoming credentials: NTLM TlRMTWNTUABAAAABIIogAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAKPBVAAAADw=
[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 TlRMTWNTUACAAAAAAAAAAAAAAAAAFgong2FwZmIo2rI4AAAAAAAAAAAAAAAAAAAA
[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/de5f23hu73ds/plugin?
target-Auth&reason-Auth&ClientID=1752291987&tl=600&url=ahR&DovL3RlC3QxbmcuY29tLw,,&nd=1658675433.155593410.d1klvarI6v8ck5jXWAtP8Kp713eHII9UtoV_otlEfs,
[2022-07-24 17:21:32.531 +02:00] [433] NTLM (132, 192.168.2.149) Configuration: User Database at Authentication Server Connection: 0x7ff804599c0 RR: 0x7ff87c01e6f0
[2022-07-24 17:21:32.531 +02:00] [433] NTLM (132, 192.168.2.149) Incoming credentials: NTLM
TlRMTWNTUADAAAGAAAYAT4AACSAkwp9AAAAADgBYAAACgAKAGYAAAAAB9A4AAAAAABSAQA0ABYklogoA8FUAAAAP/ittFvopHqjlgzjXDV2gAbwTAAAGIABHAGIAd0BzAGUAcgYAEQAR0BTAESAAVAPFA
gYmkGtHkCAB8BAQAAAAAAAH0wX5n9g8y8Tz7p4e2YAAAAACAAwAAAAAABAAAAAAGAACM3dSmD0hRvW473/DCICgkE/tAkRPUlqZwE5YKCoEAAAAAAAAAAAAAAAAAAAAAAACQAEgAVABUAFALwAA
[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 <i>logon right</i> ) 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 <b>Netlogon</b> 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 communicates via port 445 but with secure all we now see is blob data so no request or response is in clear text.

Netlogon Logs will record the request and response 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:

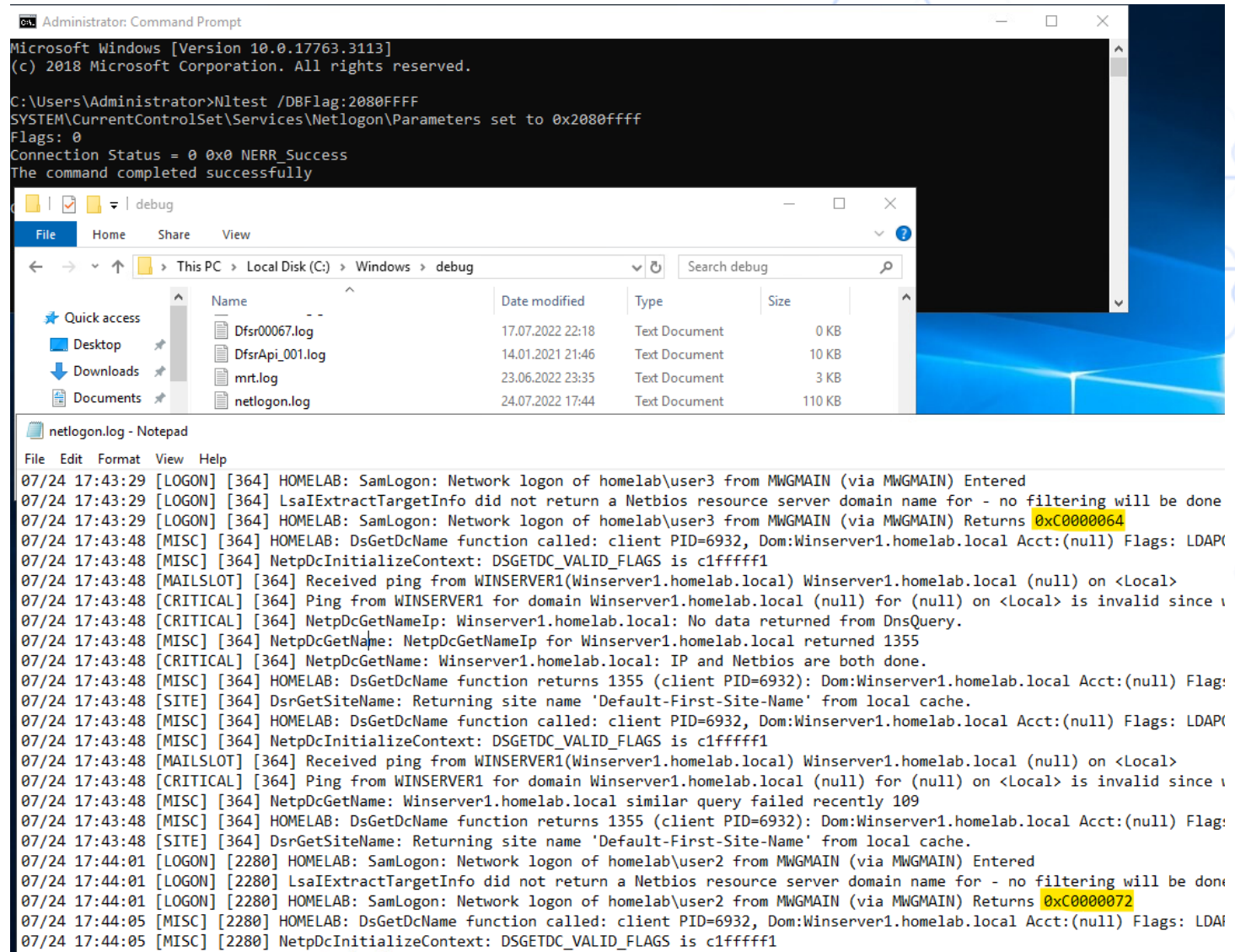
```
Nltest /DBFlag:2080FFFF
```

Disable with admin cmd prompt:

```
Nltest /DBFlag:0x0
```

Log can be found:

C Drive > Windows > Debug



The screenshot shows a Windows Administrator Command Prompt window with the following text:

```
Administrator: Command Prompt
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
```

Below the command prompt is a File Explorer window showing the contents of the 'debug' folder in 'C:\Windows\debug'. The files listed are:

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

Below the File Explorer is a Notepad window showing the contents of 'netlogon.log':

```
netlogon.log - Notepad
File Edit Format View Help
07/24 17:43:29 [LOGON] [364] HOMELAB: SamLogon: Network logon of homelab\user3 from MWGMMAIN (via MWGMMAIN) 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 MWGMMAIN (via MWGMMAIN) 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 MWGMMAIN (via MWGMMAIN) 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 MWGMMAIN (via MWGMMAIN) 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)
- MWG 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)



The screenshot shows the Alerts dashboard with the following filters: Appliance Filter (All), Date Filter (All), and Message Filter (Error, Warning, Information). Two alerts are displayed:

Appliance Filter	Date Filter	Message Filter	Type to filter alerts
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`
- Once you have determined the location you can see for example `/var/log/messages` are access logs being logged if so rsyslog config is incorrect (very common), if `connection_tracing` directory was connection traces left enabled (very common)
- `find /opt -type f -size +10000k -exec ls -alsh {} \;`

# Secure Web Gateway Troubleshooting – Common Issues Network

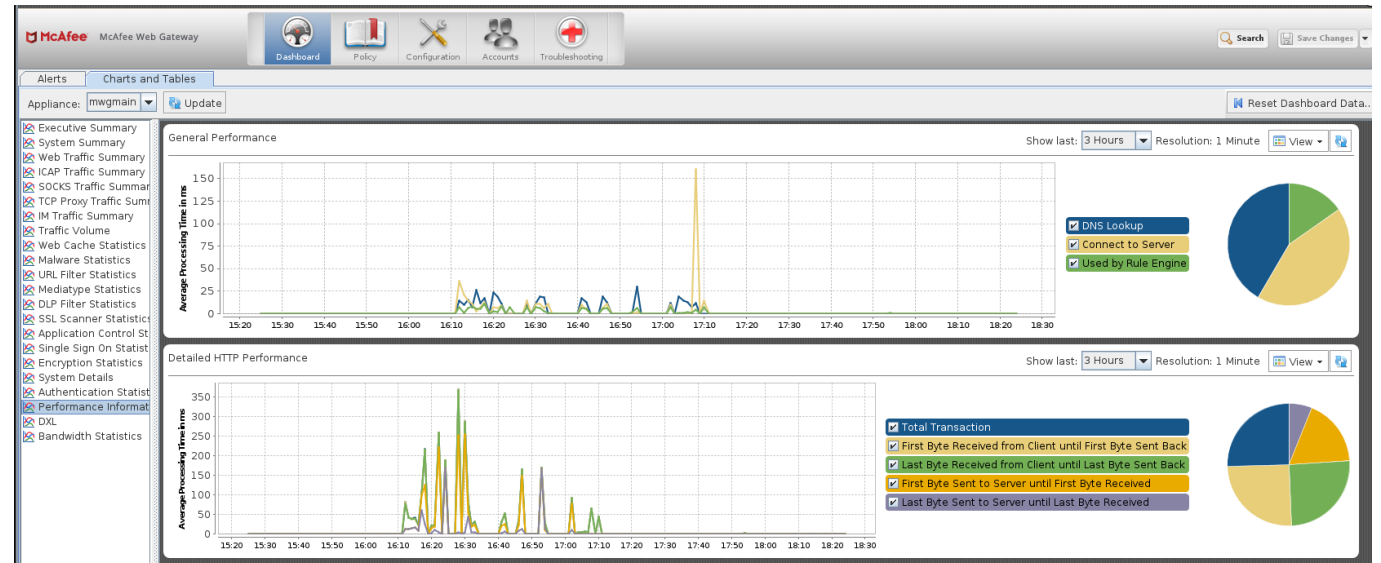
DNS, Upstream (Proxy, FW, Router, ISP, etc)

Results in:

- Delays
- SSL Handshake
- Browser Error

Page cannot be displayed  
No response

- 502 Response of MWG  
Cannot Connect  
No Response in Time  
Bad Gateway  
Host Unresolvable



# 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

Timeout when connecting  
10

Timeout when doing handshake  
15

Timeout when receiving/sending  
15

Use and Serve persistent connections

https://172.27.96.188:4712/Konfigurator/request

McAfee Web Gateway

Dashboard Policy Configuration Accounts

File Editor

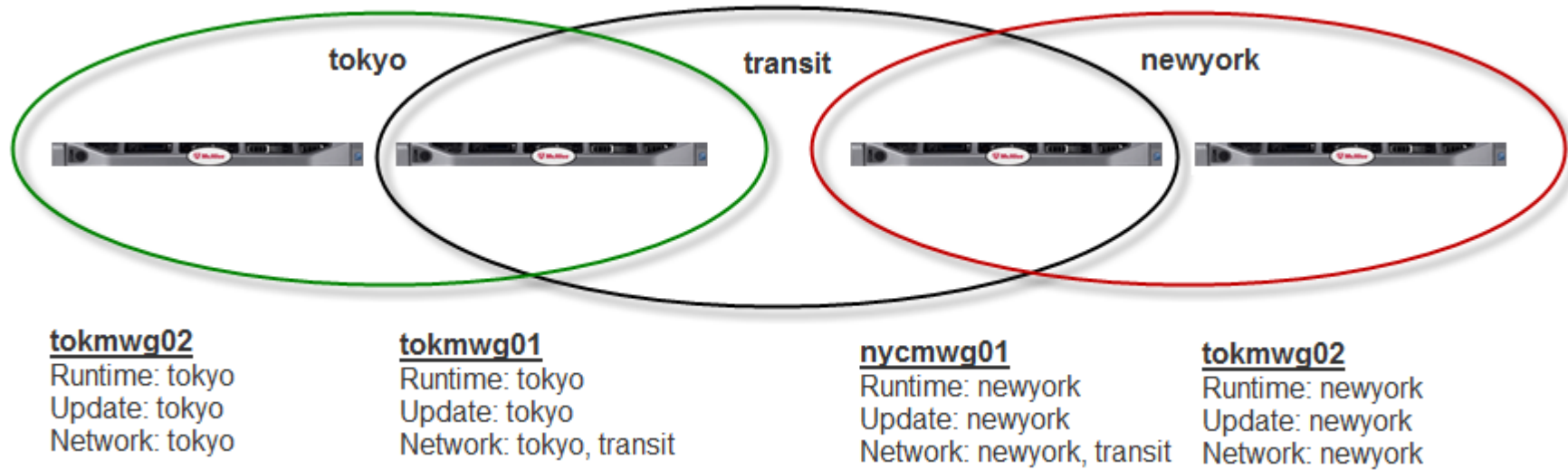
Update Engines

Central Management Settings

IP addresses and ports of this node used for central management

No.	String
1	172..27.96.188:12346

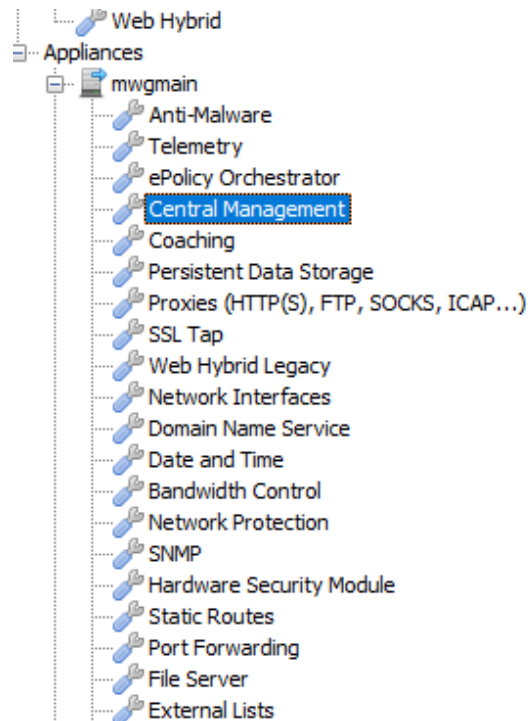
# Secure Web Gateway Troubleshooting – Common Issues Cluster - cont





# Secure Web Gateway Troubleshooting – Common Issues

## Cluster - cont



High priority (1)

Allow a GUI server to attach to this node

Allow to attach a GUI server from non local host

GUI control address (IP:port)

127.0.0.1:12344

GUI request address (IP:port)

127.0.0.1:12345

Enable IP checking for other nodes

Allowed time difference (10-600 seconds)

50

10

600

Enable version checking for other nodes

Level of version check (1-6)

1

only major release (very relaxed)

also build number must match (very strict)

Low priority (100)



# The perfect Service Request

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



Thank You!

[www.skyhighsecurity.com](http://www.skyhighsecurity.com)