

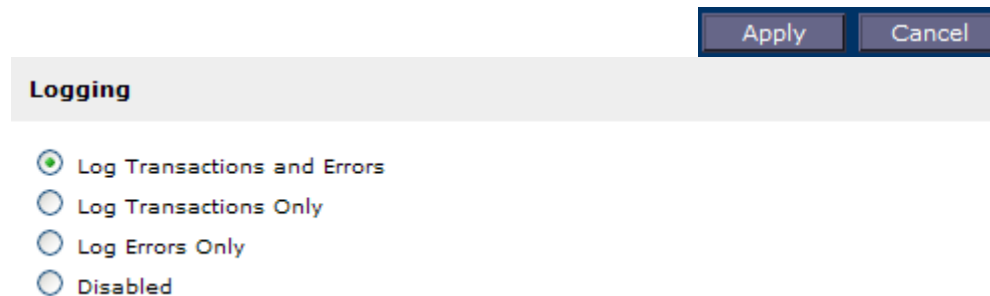
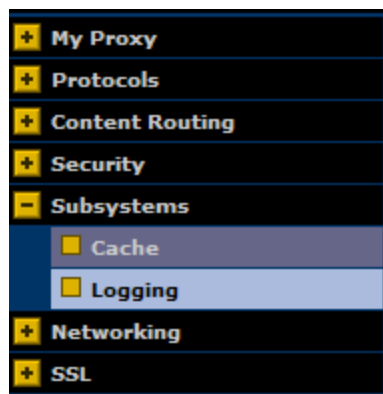
Troubleshooting and Debugging Strategies for V-Series v7.5

Support Webinars

- Understanding Content Gateway (proxy) extended.log
 - What is extended.log
 - Turning on extended.log
 - Viewing extended.log – what do the fields mean?
 - Examples: HTTP request; NTLM messages; HTTPS decryption
- The new V-Series Toolbox
 - Understanding the IP addressing structure of the V-Series
 - Using TCPDump
 - A real-world example using TCPDump
 - Using Wget to test URLs
- Debugging in the Content Gateway module
 - Enabling debug through the new V-Series Toolbox
 - Debug examples for specific issues
 - Accessing debug information
 - **Making sure that debug output is turned off**

Understanding extended.log

- What is extended.log?
 - Accumulates a record of traffic going through the proxy
 - Is turned off by default
 - When is an entry added to extended.log?
 - Turning on extended.log



Understanding extended.log

- How to view extended.log:
 - Viewing in the Content Gateway Manager GUI
 - Go to: Configure > My Proxy > Logs and then the Access tab

The screenshot displays the Content Gateway Manager GUI. On the left, a sidebar menu shows 'My Proxy' expanded, with 'Logs' selected. The main content area shows the 'Access Logs' section. Under 'Log File', a dropdown menu is open, showing 'extended.log [3.9 KB]' as the selected file. Below the dropdown, there are five radio button options for displaying the log file:

- Display the selected log file
- Display last lines of the selected file
- Display lines that match in the selected log file
- Remove the selected log file
- Save the selected log file in local filesystem

Understanding extended.log

- extended.log field descriptions:

```
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/EUROPE/potd/2001/04/17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473 000 0 0 0 458 297 0 0 0
```

Diagram illustrating the fields in an extended.log entry:

- 1: IP address of the client's host machine (209.131.54.138)
- 2: Hyphen (-)
- 3: Authenticated client user name (-)
- 4: Date and time of the client's request, enclosed in brackets ([17/Apr/2001:16:20:28 -0700])
- 5: Requested URL, enclosed in quotes ("GET http://europe.cnn.com/EUROPE/potd/2001/04/17/tz.pullitzer.ap.jpg HTTP/1.0")
- 5 cont'd: Continuation of the requested URL
- 6: Proxy response status code (200)
- 7: Length of the Content Gateway response to the client in bytes (4473)
- 8: Origin server's response status code (000)
- 9: Server response transfer length; the body length in the origin server's response to the proxy, in bytes (0)
- 10: (0)
- 11: (0)
- 12: Time Content Gateway spent processing the client request; the number of seconds between the time that the client established the connection with the proxy and the time that the proxy sent the last byte of the response back to the client (458)
- 13: (297)
- 14: (0)
- 15: (0)
- 16: (0)

Field	Description
1	The IP address of the client's host machine.
2	This hyphen (-) is always present in Netscape log entries.
3	The authenticated client user name. A hyphen (-) means no authentication was required.
4	The date and time of the client's request, enclosed in brackets.
5	The requested URL, enclosed in quotes.
6	The proxy response status code (HTTP reply code).
7	The length of the Content Gateway response to the client in bytes.
8	The origin server's response status code.
9	The server response transfer length; the body length in the origin server's response to the proxy, in bytes.
16	The time Content Gateway spent processing the client request; the number of seconds between the time that the client established the connection with the proxy and the time that the proxy sent the last byte of the response back to the client.

Details can be found in Content Gateway Online Help by searching for "extended.log".

Understanding extended.log

extended.log examples:

- Successful HTTP GET request:

```
10.0.0.1 - - [06/Jul/2010:11:51:07 -0000] "GET http://www.websense.com/content/home.aspx HTTP/1.0" 200 64384 200 64384 0 0 204 250 233 222 0
```

- NTLM authentication interaction:

```
10.0.0.2 - - [06/Jul/2010:11:54:20 -0000] "GET http://www.google.co.uk/ HTTP/1.1" 407 322 000 0 0 0 581 309 0 0 0
```

```
10.0.0.2 - - [06/Jul/2010:11:54:20 -0000] "GET http://www.google.co.uk/ HTTP/1.1" 407 322 000 0 0 0 665 306 0 0 0
```

```
10.0.0.2 - USER1 [06/Jul/2010:11:54:20 -0000] "GET http://www.google.co.uk/ HTTP/1.1" 200 6076 200 6076 0 0 906 264 677 236 0
```

- Websense Block message:

```
10.0.0.3 - - [06/Jul/2010:11:57:55 -0000] "GET http://www.playboy.com/ HTTP/1.0" 302 0 000 0 0 0 133 187 0 0 0
```

```
10.0.0.3 - - [06/Jul/2010:11:57:55 -0000] "GET http://10.0.0.20 1:15871/cgi-bin/blockpage.cgi?ws-session=687865857 HTTP/1.0" 200 1505 200 1505 0 0 141 144 170 118 0
```

Understanding extended.log

extended.log examples (continued):

- Showing HTTPS decryption:

10.5.144.32 - [12/Jul/2010:15:43:51 -0000] "CONNECT www.cia.gov:443/ HTTP/1.0" 200 127 200 0 0 0 383 127 542 76 0

10.5.144.32 - - [12/Jul/2010:15:43:52 -0000] "GET http://www.cia.gov/javascript/register_function-cachekey1018.js
HTTP/1.1" 200 52663 200 52663 0 0 840 297 829 287 0

10.5.144.32 - - [12/Jul/2010:15:43:53 -0000] "GET http://www.cia.gov/css/IEFixes.css HTTP/1.1" 200 3642 200 3642 0 0 810
279 799 269 0

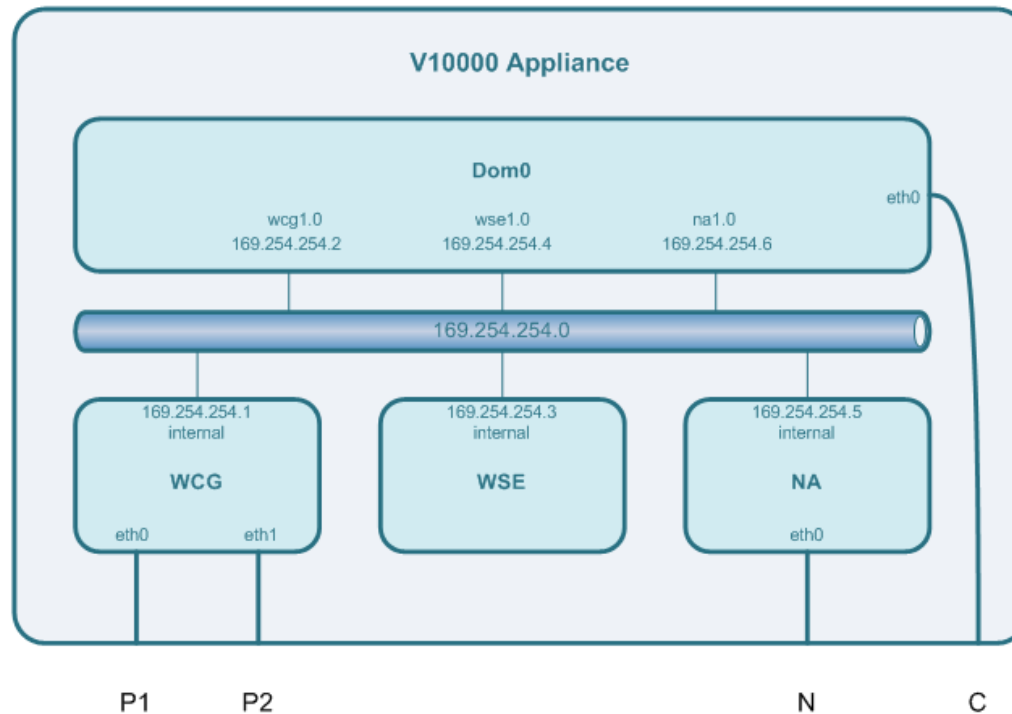
10.5.144.32 - - [12/Jul/2010:15:43:53 -0000] "GET http://www.cia.gov/css/ciatheme-index.css HTTP/1.1" 200 10657 200
10657 0 0 818 281 807 271 0

10.5.144.32 - - [12/Jul/2010:15:43:53 -0000] "GET http://www.cia.gov/css/base-cachekey6837.css HTTP/1.1" 200 59571 200
59571 0 0 821 281 810 271 0

10.5.144.32 - - [12/Jul/2010:15:43:53 -0000] "GET http://www.cia.gov/javascript/javascript.js HTTP/1.1" 200 6092 200 6092
0 0 820 296 809 286 0

The New V-Series Toolbox

- Understanding the IP addressing structure of the V-Series to aid in analyzing packet captures



The New V-Series Toolbox

■ Using TCPDump

- Located in the new 7.5 V-Series user interface:

WEBSense® V10000 Log Off

Administration > Toolbox ? Help Apply Changes

Command Line Utility i

Execute basic network troubleshooting commands for appliance modules in a command line environment.

Launch Utility

Technical Support Tools i

Troubleshooting Ports

Enable troubleshooting ports temporarily when requested by Websense Technical Support.

Enable troubleshooting ports Save

Appliance Configuration Summary

The configuration summary tool gathers data from the appliance and generates a file that can be sent to Websense Technical Support for analysis and debugging. This will take approximately 1-2 minutes.

Generate File

Remote Access

Enable remote access only at the request of Websense Technical Support. When remote access is enabled, a passcode is automatically generated. Provide the passcode to the support technician.

Enable Remote Access
Passcode: **mryJ53** Save

Remote access logon history:

Session Start	Session End	Connected From

The New V-Series Toolbox

- Select the appliance module on which the command will be run
- Then select the command you want to run

https://10.212.1.45:9447/appmng/configuration/CommandLine.jsf - Windows Internet Explorer

Command Line Utility

The command line utility provides the ability to execute various network debugging commands that are run from any appliance module.

Module:

Command:

- content_line -r
- content_line -s
- content_line -x
- ethtool
- ethtool -k
- ifconfig
- nc -uvz
- nc -vz
- netstat -neatup
- netstat -ng
- netstat -nitup
- netstat -s
- nslookup
- ping
- ping -l
- print_bypass
- route -n
- sysctl_tcp_timestamps
- sysctl_tcp_window_scaling
- tcpdump
- tcpdump -w
- top -bn1
- traceroute
- wcg_net_check
- wget

Console output:

```
ts-v10000-G2 (Websense Content Gateway)#
```

[Download output file for last command](#)

The New V-Series Toolbox

- For TCPDump, you can select “tcpdump -w” to dump output to a .cap file.
 - Select the interface to run the capture on: P1, P2, eth0 (P1), eth1 (P2)
Or select the “any” option
 - In the Expression entry field, enter the expression you want to capture. There are numerous expressions, including “and” and “or” statements.
For example: port 80 or port 8080
 - Press **Run** to start the capture

Module: ▼

Command: ▼

tcpdump -w

Write the raw packets to a downloadable file.

Interface:
Only interface(s) associated with selected module are permitted. ⓘ

Expression:
Filter which packets are displayed ⓘ

The New V-Series Toolbox

- When you have finished reproducing the issue, click to **Stop** the capture

Module:

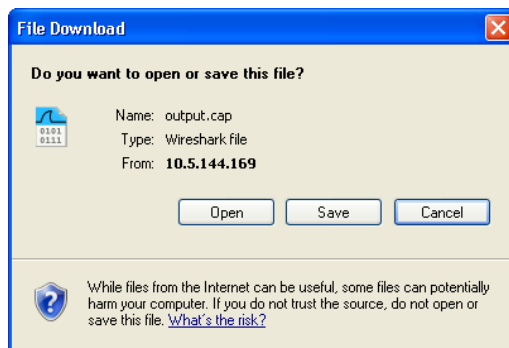
Command:

tcpdump -w
Write the raw packets to a downloadable file.

Interface:
Only interface(s) associated with selected module are permitted. [i](#)

Expression:
Filter which packets are displayed [i](#)

- You can download the file to your machine to view with Wireshark, for example



Console output:

```
uklab-v10k3 (Websense Content Gateway)#tcpdump -w output.cap -c 1000
0 -s 0 -i p1 -l port 8080
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535
bytes
0 packets captured
0 packets received by filter
0 packets dropped by kernel

uklab-v10k3 (Websense Content Gateway)#
```

[Download output file for last command](#)



- Real-world example of TCPDump
 - Enable TCPDump to look at:
 - Incoming traffic from a client machine
 - Outgoing traffic from the proxy to the Internet
 - DNS traffic
 - Start the capture
 - Set a client machine to browse through the proxy
 - Stop the capture
 - Download the file
 - Open the file in Wireshark

The New V-Series Toolbox

- Using Wget to test URLs by bypassing the proxy
 - Wget makes a request to the end URL and attempts to download index.html from the site
 - As with the TCPDump select the Appliance module you wish to run the Wget from.
 - Choose Wget from the list
 - Then enter the URL you wish to test
 - Press Run



```
uklab-v10k3 (Websense Content Gateway)#wget -t 3 --progress=dot --no-check-certificate --delete www.google.com
--13:17:43-- http://www.google.com/
Resolving www.google.com... 66.102.9.103, 66.102.9.106, 66.102.9.104, ...
Connecting to www.google.com[66.102.9.103]:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://www.google.co.uk/ [following]
--13:17:43-- http://www.google.co.uk/
Resolving www.google.co.uk... 66.102.9.106, 66.102.9.104, 66.102.9.147, ...
Reusing existing connection to www.google.com:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `index.html&apos;

OK ..... 244K=0.03s

13:17:43 (244 KB/s) - `index.html&apos; saved [8463]

Removing index.html.

uklab-v10k3 (Websense Content Gateway)#
```

Module: 
Command: 

wget

Verify connectivity with specified URL (file download not supported)


URL:


Run

Stop

■ Wget Example of a failure

- Example of a DNS failure for a site:

Module: 

Command: 

wget

Verify connectivity with specified URL (file download not supported)

URL:

Run

Stop

```
uklab-v10k3 (Websense Content Gateway)#wget -t 3 --progress=dot --no-check-certificate --delete www.wibble.com
--14:07:14-- http://www.wibble.com/
Resolving www.wibble.com... failed: Temporary failure in name resolution.

uklab-v10k3 (Websense Content Gateway)#
```

In this example the site will not work through the proxy as the DNS for the site is failing therefore the proxy will not be able to make the outbound connection on behalf of the user

Debugging in the proxy module

- The new V-Series Toolbox allows users to run proxy configuration commands
- To enable Debug output you need to add two lines to the configuration file with some variables:
 - *proxy.config.diags.debug.tags*
 - *proxy.config.diags.debug.enabled*
 - The first selects the debug tags that you want to enable
 - The second turns debug output on or off
- Using the V-Series Toolbox, select the Content Gateway module and then select “*content_line -s*”
- Set the debug tags you want to use:

content_line -s

Assign the Content Gateway configuration variable a specified value. See [records.config](#) for a list of configuration variables.

Variable Name:

Value:

Debugging in the proxy module

- Turn debug output on:

content_line -s

Assign the Content Gateway configuration variable a specified value. See [records.config](#) for a list of configuration variables.

Variable Name:

Value:

- Cause the proxy to read the new configuration settings:

Module: ▼

Command: ▼

content_line -x

Immediately apply all configuration changes made with *content_line -s* or Content Gateway Manager. No restart of Websense Content Gateway required.

Debugging in the proxy module

■ When you're done, make sure you turn debug output off!

- Again use the Toolbox “content_line -s” command and set the “proxy.config.diags.debug.enabled” to a value of 0

content_line -s

Assign the Content Gateway configuration variable a specified value. See [records.config](#) for a list of configuration variables.

Variable Name:

Value:



- Then use “content_line -x” to apply the changes:

content_line -x

Immediately apply all configuration changes made with *content_line -s* or Content Gateway Manager. No restart of Websense Content Gateway required.

Debugging in the proxy module

- You can also check the value of the enabled flag in the configuration:
 - Use the “content_line -r” command to check whether the debug is:
 - Enabled (the value is 1)
 - Disabled (the value is 0)

Module: 
Command: 

content_line -r
Display the value of the specified Content Gateway variable. See [Websense Content Gateway variables](#) for a list of variables.

Variable Name:

Console output:

```
uklab-v10k3 (Websense Content Gateway)#content_line -r proxy.config.diags.debug.enabled
1
uklab-v10k3 (Websense Content Gateway)#
```

Debugging in the proxy module

- Accessing the debug file
 - All debug information is logged to the “content_gateway.out” file
 - The file is accessed in the Logs section of the V-Series GUI
 - You can view the logs in the GUI, or by downloading the file to another computer

Logs i

Websense Technical Support may request log files to assist you with unexpected results.

Select Module:

- Appliance Controller
- Websense Content Gateway**
- Websense Web Security
- Network Agent

Websense Content Gateway Log Options

View options: View last lines

Download entire log file

■ Debugging Examples:

- Debugging NTLM authentication when a User is unable to login
 - Debug tags = ntlm.*
- Debugging DNS
 - Debug tags = dns.* | hostdb.*
- Debugging HTTP headers and Websense Filtering Plugin
 - Debug tags = http_hdrs.* | wtg_txn.*

- Best practices:
 - Only turn on debug output when trying to debug specific problems
 - Consider devising a test that reproduces the problem and turn on debug output just before starting the test
 - Make sure that the debug output is turned off when you are finished
 - If you are in any doubt about the configuration settings, go back to the Toolbox and check with “content_line -r”

Support Online Resources

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

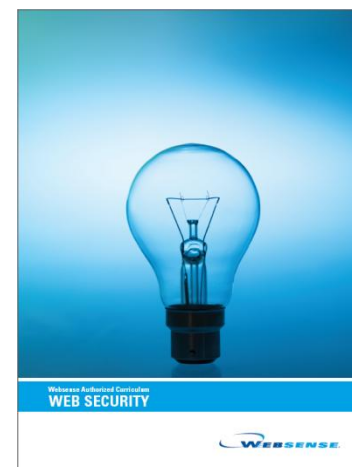
- Create and manage support service requests using our online portal.

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:
<http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:
readiness@websense.com

WEBSense®
**Authorized Training
Partner**

WEBSense®
Certified Instructor



Webinar Update

Spanish Webinar:

Title: Implementation and Configuration of Websense
Web Security Gateway v7.5

Date: July 28, 2010

Time: 8:30 A.M. PDT (GMT -7)

English Webinar:

Title: Configuring and Troubleshooting Websense
Solutions for Filtering Off-Site Users

Date: August 25, 2010

Time: 8:00 A.M. PDT (GMT -7)

How to register:

[http://www.websense.com/content/
SupportWebinars.aspx](http://www.websense.com/content/SupportWebinars.aspx)

Questions?

websense[®]
ESSENTIAL INFORMATION PROTECTION™

