

Quick Start 4: Identifying and Troubleshooting proxy issues for Websense Web Security Gateway

Websense Support Webinar March 2013

TRITON™

Web security

Email security

Data security

Mobile security

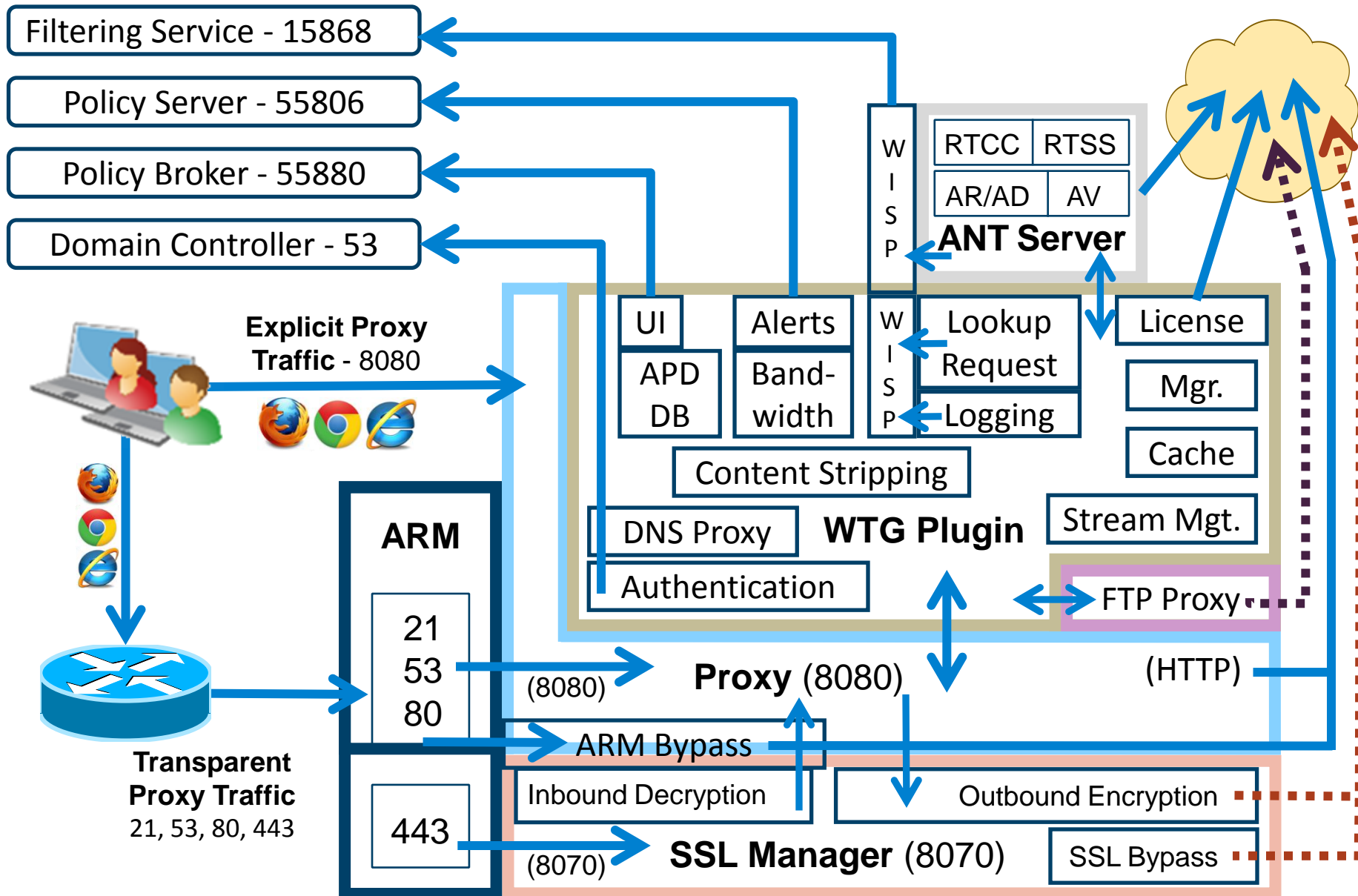


Greg Didier

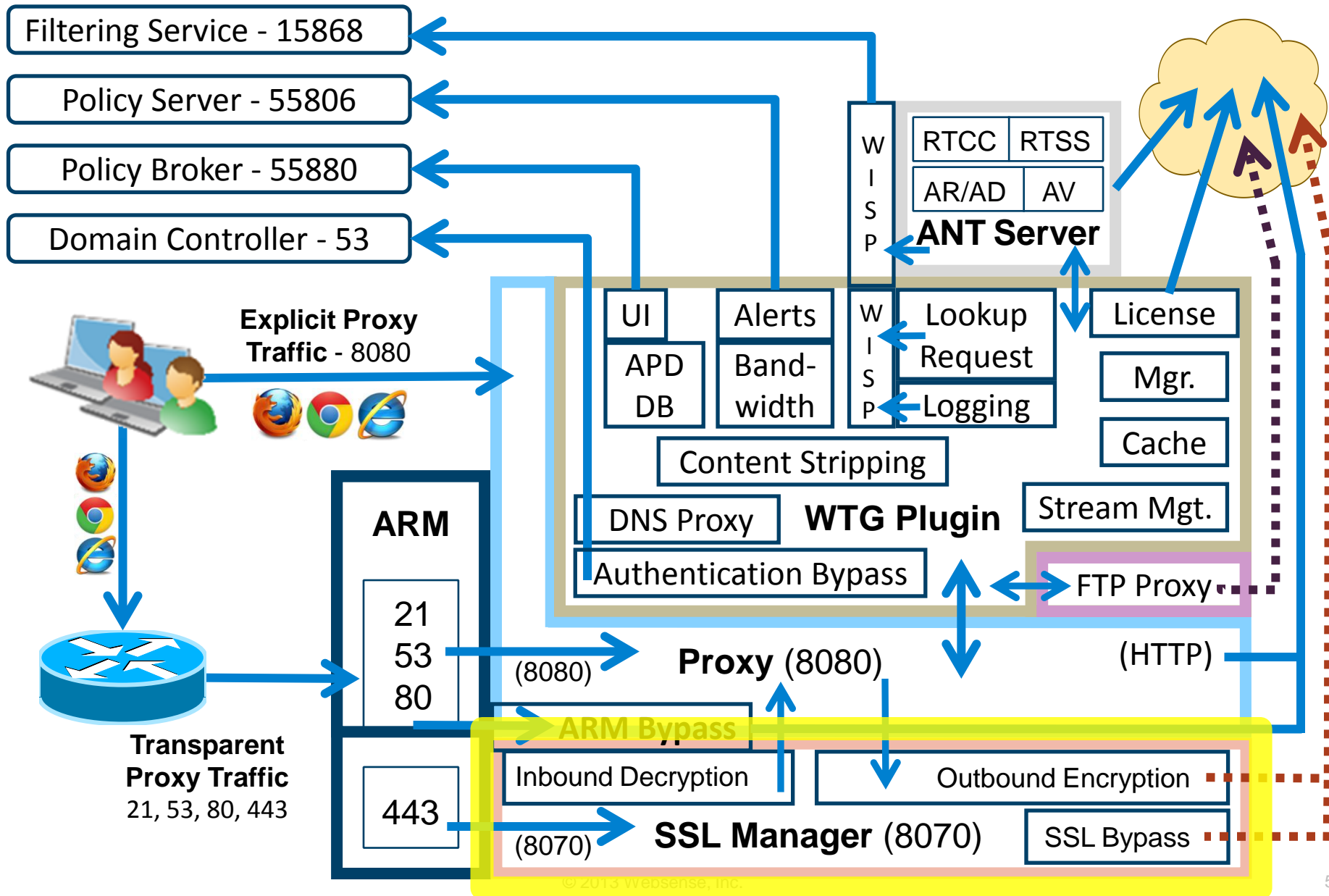
- **Title:**
 - Support Specialist
- **Accomplishments:**
 - 9 years supporting Websense products
- **Qualifications:**
 - Technical Support Mentor
 - Product Trainer

- Traffic flow
- Components and processes
- Configure logging
- Identify relevant log files
- How to resolve issue
 - Exceptions
 - Bypassing
 - Tunneling
- After this webinar, you will understand how the proxy works and know where available resources are to resolve issues

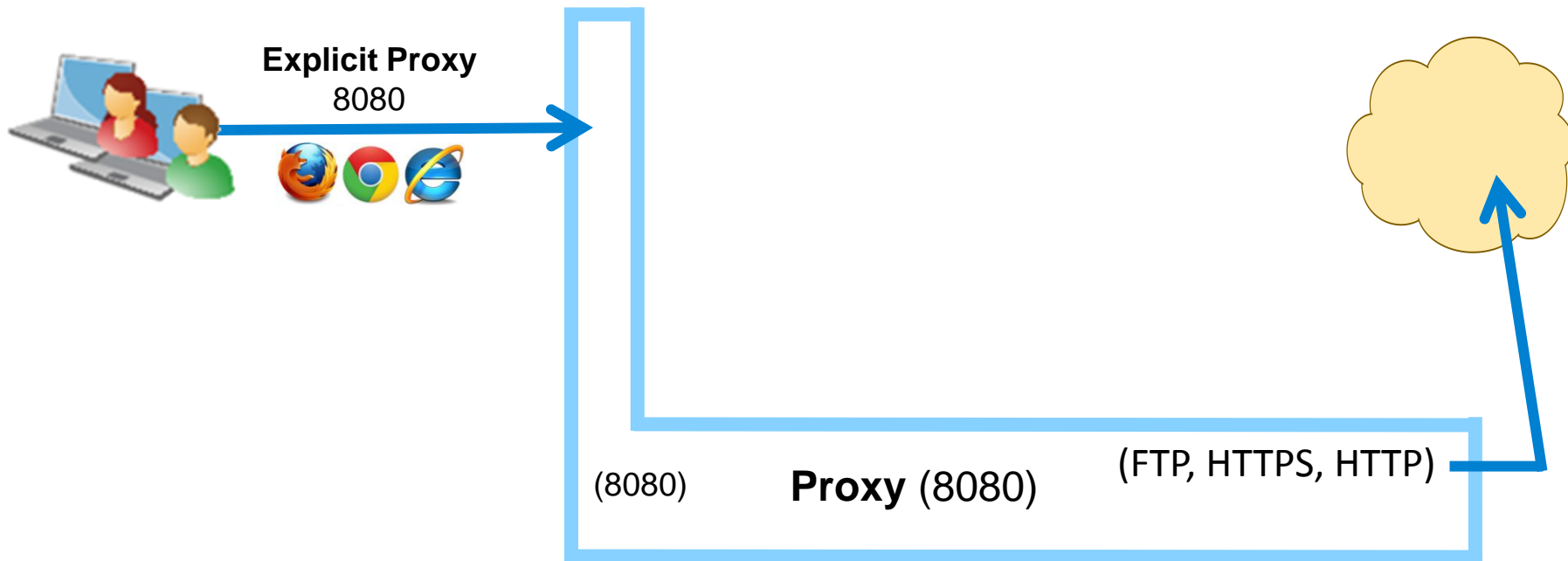
Content Gateway Traffic Flow



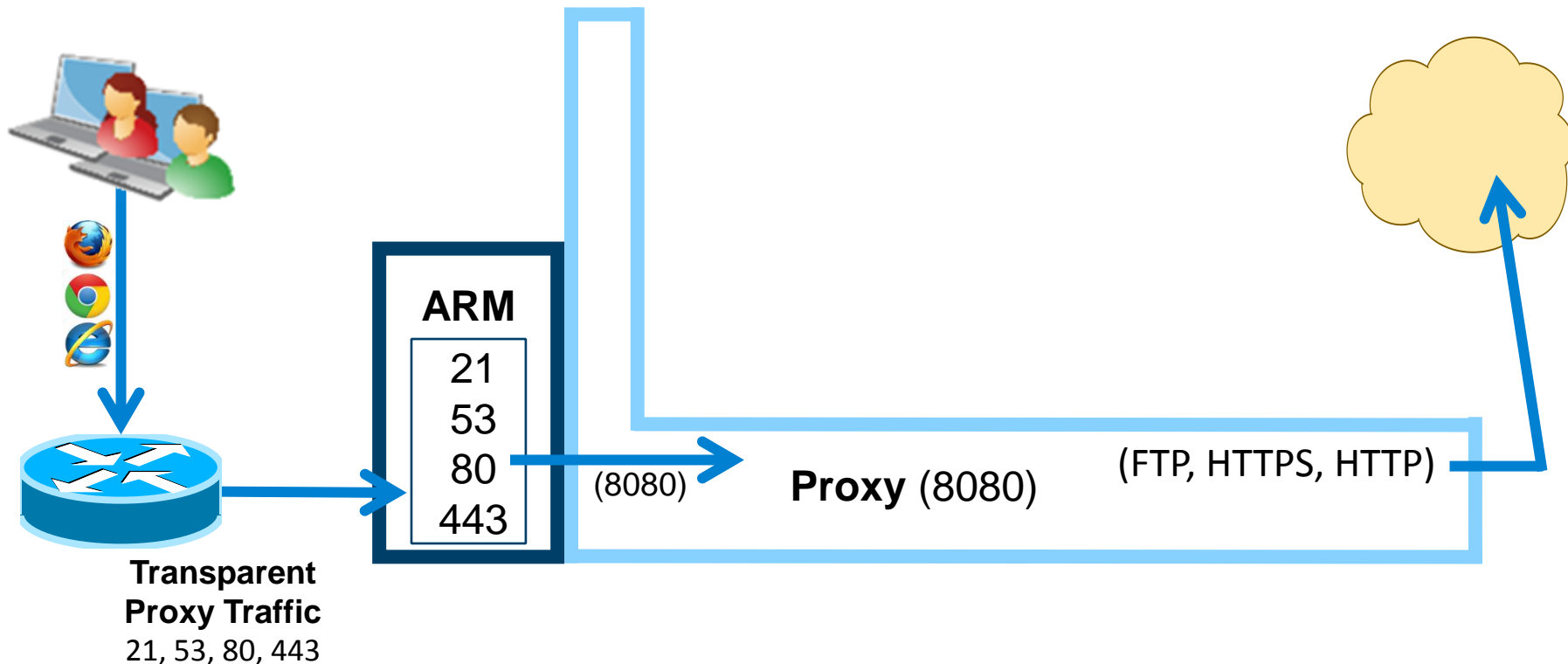
SSL Manager



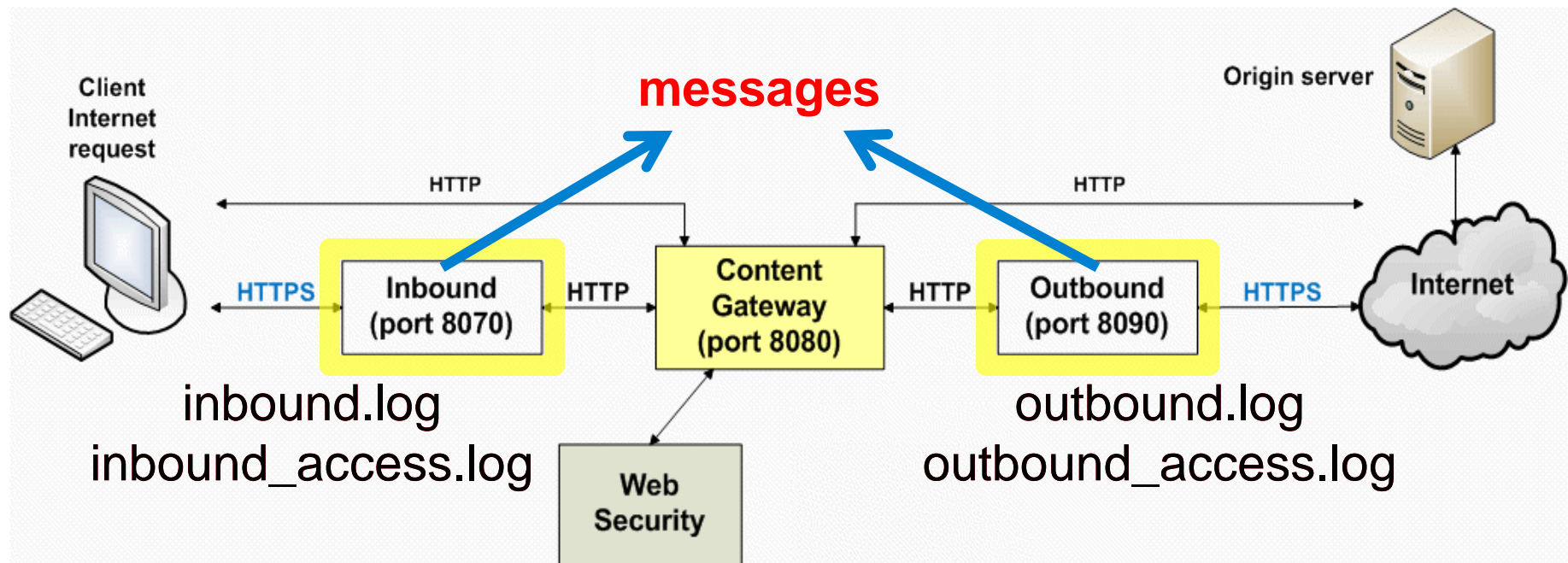
- Explicit proxy
 - Browser is aware of the proxy
 - URL filtering based on Host name in the request



- Transparent proxy
 - Browser is not aware of the proxy
 - URL filtering based on Common Name in certificate



- Capturing logging data
 - Inbound transactions to SSL Manager from client
 - Outbound transactions to origin server from SSL Manager
 - Alternatively, you may send SSL inbound and outbound logging data to the system *messages* file



- Provides SSL decryption
- Requires deploying certificates
- Troubleshooting
 1. Configure SSL logging
 - Select Configure > SSL > Logging > General tab
 - Enable all logs, set logging level to 7, enable syslog, enable File and apply changes

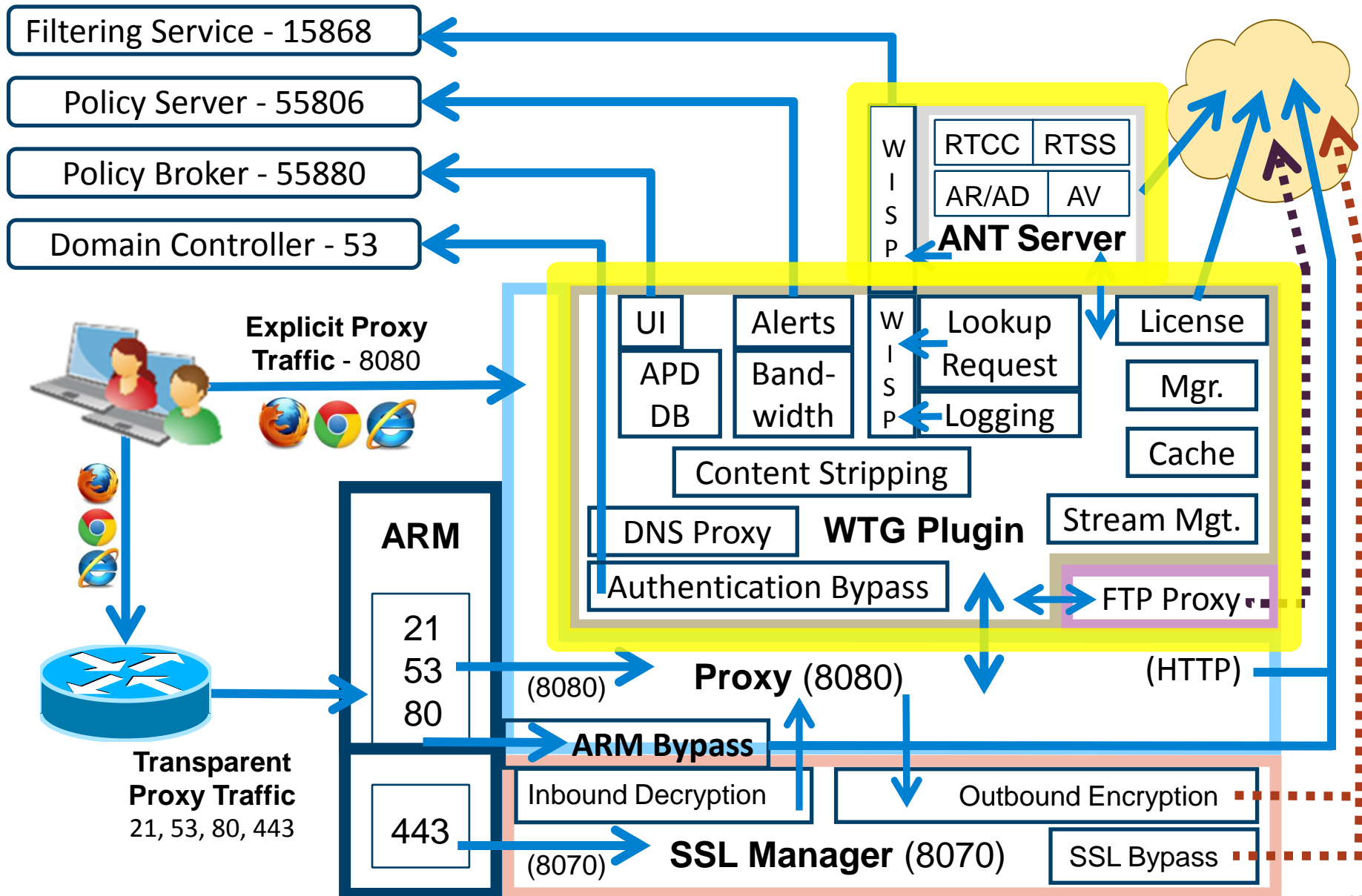
Inbound	<input checked="" type="checkbox"/> Logging level <input type="text" value="7"/>	<input checked="" type="checkbox"/> syslog	<input checked="" type="checkbox"/> File	Filename: inbound.log
	<input checked="" type="checkbox"/> Access log file	<input checked="" type="checkbox"/> syslog	<input checked="" type="checkbox"/> File	Filename: inbound_access.log
Outbound	<input checked="" type="checkbox"/> Logging level <input type="text" value="7"/>	<input checked="" type="checkbox"/> syslog	<input checked="" type="checkbox"/> File	Filename: outbound.log
	<input checked="" type="checkbox"/> Access log file	<input checked="" type="checkbox"/> syslog	<input checked="" type="checkbox"/> File	Filename: outbound_access.log

2. Reproduce the issue

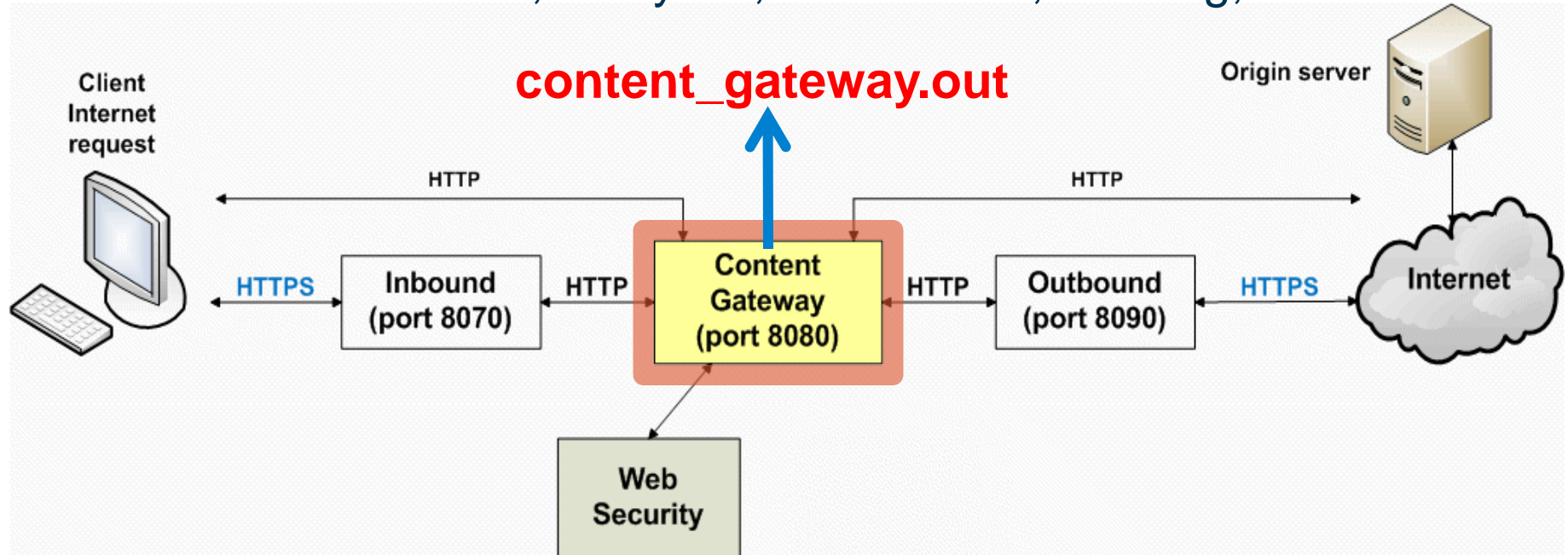
- Troubleshooting (continued)
 3. Examine SSL Manager logs
 - In the Content Gateway console
 - Select Configure > My Proxy > Logs > System tab > Log File > *messages*
 - Alternatively, SSH client to `/opt/WCG/sxsuite/log/`
 - *inbound.log, inbound_access.log*
 - » Client connection to SSL Manager
 - *outbound.log, outbound_access.log*
 - » SSL Manager connection to destination server
 4. Disable SSL logging
- Demonstration

- Viewing SSL logs is a four step process
 1. Configure SSL logging
 2. Reproduce issue
 3. Examine SSL Manager logs
 - In the *messages* log
 4. Disable SSL logging

Analytic And Process Transactions



- Capturing logging data
 - Content Gateway is the workhorse for analyzing traffic and enforcing security policies
 - Capturing transaction requires enabling debugging tags for specific processes, such as:
 - Authentication, analytics, virus scans, caching, etc.

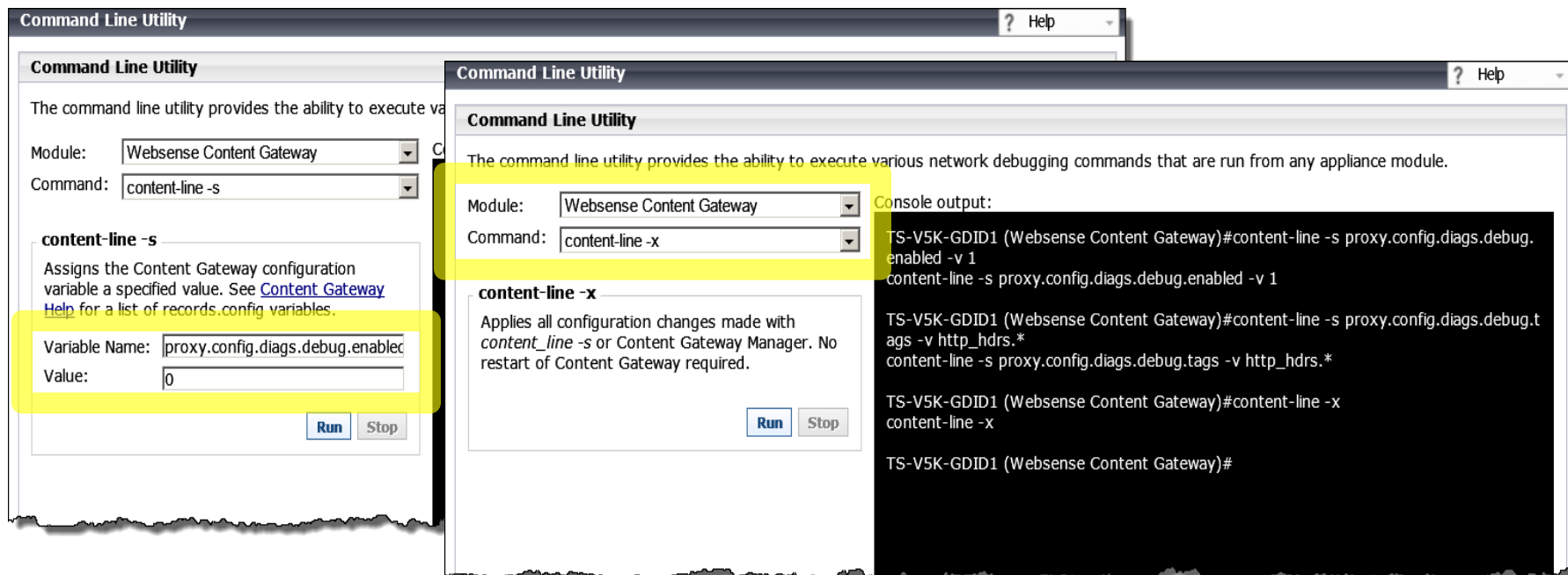


- Debug tags enable logging for specific processes
 - Enabled via command line
- Only *content_gateway.out* receives tag logging data
 - Displayable within the Content Gateway console
- Avoid editing the *records.config* file
 - While in the `/opt/WCG/bin/` directory, best practice is adding entries via the `content_line` command
 - If the Content Gateway bin directory is not in your path, prepend the command with `./`. For example: `./content_line`
- Steps to capture logging data:
 1. Enable logging
 2. Specify interesting tags
 3. Apply changes
 4. Reproduce issue and view logs
 5. Disable logging

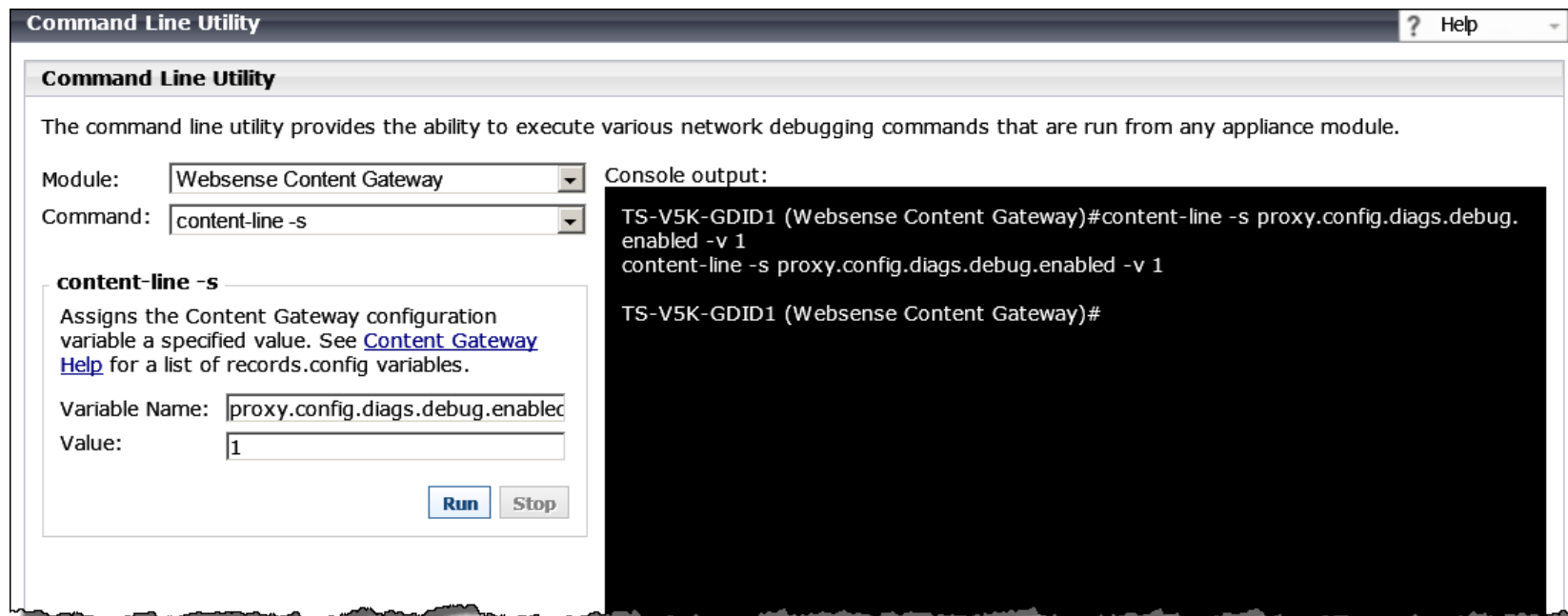
- From the /opt/WCG/bin/ directory
 1. Enable debug logging
 - `content_line -s proxy.config.diags.debug.enabled -v 1`
 2. Enable one or more debug tags
 - `content_line -s proxy.config.diags.debug.tags -v "win.*|ntlm.*"`
 - Logs IWA and NTLM authentication activity.
 3. Reload the configuration to apply changes
 - `content_line -x`
 4. Reproduce the issue and review debugging data
 - Content Gateway console, select Configure > My Proxy > Logs > System tab > Log File > *content_gateway.out*
 - `tail -f /opt/WCG/logs/content_gateway.out`
 5. Disable debug logging
 - `content_line -s proxy.config.diags.debug.enabled -v 0`
 - `content_line -x`

- Common debug logging tags
 - DNS Proxy
 - `hostdb.*`
 - SSL Manager events
 - `ssl.*` or `http_ssl.*`
 - HTTP Proxy
 - `http_hdrs.*`
 - FTP Proxy
 - `ftp.*`
 - Analytics (RTCC, RTSS, AR, AD, AV)
 - `wtg_txn.*`
 - General tag to log real-time activities
 - Authentication
 - `win.*` or `ldap.*` or `ntlm.*`
- Demonstration

- **WARNING:** Log files can become very large. Do not leave debug logging enabled.
 - On software installations, from the /opt/WCG/bin/ folder run:
 - `content_line -s proxy.config.diags.debug.enabled -v 0`
 - `content_line -x`
 - On a V-series appliance, run:



1. Enable debug logging



The screenshot shows the 'Command Line Utility' window. It has a title bar with a question mark and 'Help'. The main area is titled 'Command Line Utility' and contains a description: 'The command line utility provides the ability to execute various network debugging commands that are run from any appliance module.' Below this, there are two dropdown menus: 'Module:' set to 'Websense Content Gateway' and 'Command:' set to 'content-line -s'. To the right of these is a 'Console output:' section with a black background and white text showing the command execution: 'TS-V5K-GDID1 (Websense Content Gateway)#content-line -s proxy.config.diags.debug.enabled -v 1' and 'content-line -s proxy.config.diags.debug.enabled -v 1'. Below the dropdowns, there is a section for 'content-line -s' with a description: 'Assigns the Content Gateway configuration variable a specified value. See [Content Gateway Help](#) for a list of records.config variables.' This section has two input fields: 'Variable Name:' set to 'proxy.config.diags.debug.enabled' and 'Value:' set to '1'. At the bottom right of this section are 'Run' and 'Stop' buttons.

Command Line Utility

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

Module: Websense Content Gateway

Command: content-line -s

content-line -s

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

Variable Name: proxy.config.diags.debug.enabled

Value: 1

Run Stop

Console output:

```
TS-V5K-GDID1 (Websense Content Gateway)#content-line -s proxy.config.diags.debug.enabled -v 1
content-line -s proxy.config.diags.debug.enabled -v 1

TS-V5K-GDID1 (Websense Content Gateway)#
```

- **Module:** Websense Content Gateway
- **Command:** content-line -s
- **Variable Name:** proxy.config.diags.debug.enabled
- **Value:** 1
- Run

2. Enable one or more debug tags

The screenshot shows the 'Command Line Utility' window. It has a title bar with a question mark and 'Help'. The main area is titled 'Command Line Utility' and contains the text: 'The command line utility provides the ability to execute various network debugging commands that are run from any appliance module.'

Module:

Command:

content-line -s

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

Variable Name:

Value:

Console output:

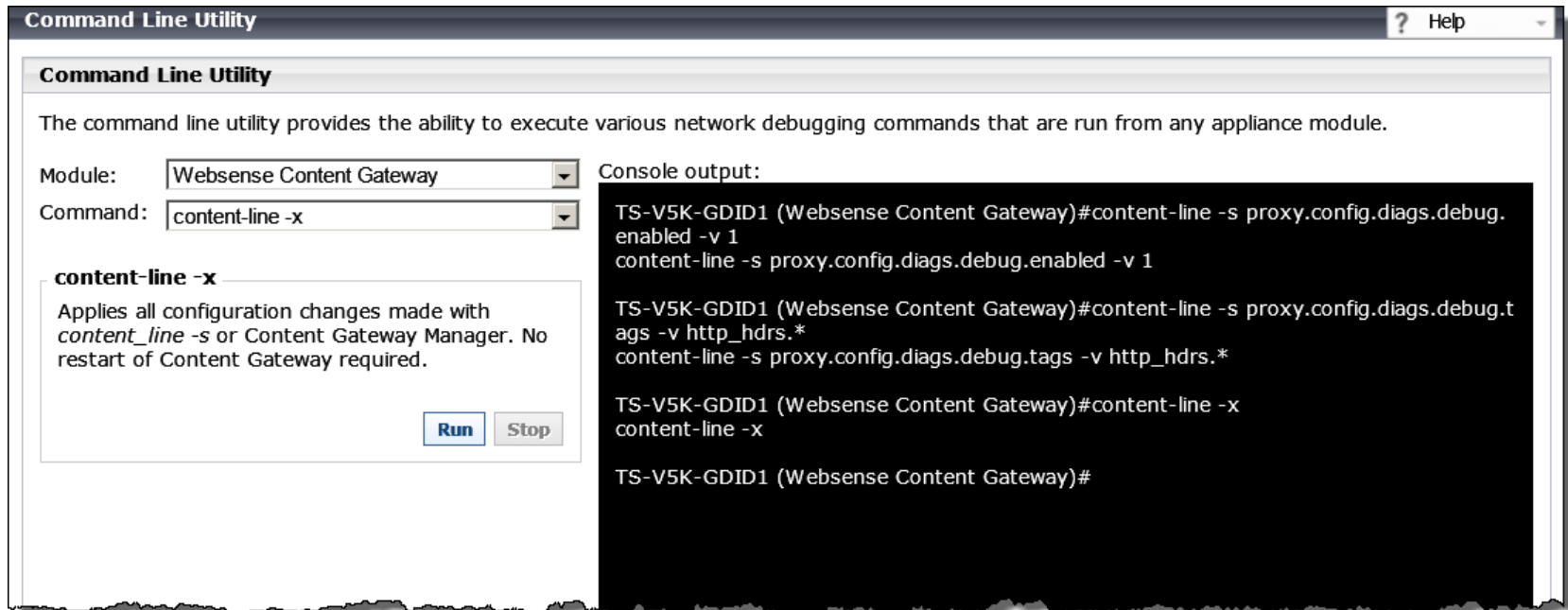
```
TS-V5K-GDID1 (Websense Content Gateway)#content-line -s proxy.config.diagnostics.debug.enabled -v 1
content-line -s proxy.config.diagnostics.debug.enabled -v 1

TS-V5K-GDID1 (Websense Content Gateway)#content-line -s proxy.config.diagnostics.debug.tags -v http_hdrs.*
content-line -s proxy.config.diagnostics.debug.tags -v http_hdrs.*

TS-V5K-GDID1 (Websense Content Gateway)#
```

- **Module:** Websense Content Gateway
- **Command:** content-line -s
- **Variable Name:** proxy.config.diagnostics.debug.tags
- **Value:** http_hdrs.*
- Run

3. Reload configuration to apply changes



- **Module:** Websense Content Gateway
- **Command:** content_line -x
- Run

4. Reproduce issue and review debugging data

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes the 'Monitor' and 'Configure' tabs, with 'Configure' being the active tab. The user is logged in as 'admin'. The left sidebar contains a tree view of configuration categories: My Proxy, Basic, Subscription, UI Setup, Snapshots, Logs (selected), Protocols, Content Routing, Security, Subsystems, Networking, and SSL. The main content area is divided into 'System' and 'Access' sections. The 'System' section is active, showing 'System Logs' and an 'Apply' button. Below this, the 'Log File' section is highlighted with a red circle, showing a dropdown menu with 'content_gateway.out [13.4 KB]' selected. The 'Action' section below it contains five radio button options: 'Display the selected log file', 'Display last 100 lines of the selected file' (selected), 'Display lines that match [] in the selected log file', 'Remove the selected log file', and 'Save the selected log file in local filesystem'. At the bottom, a text area displays the log content, starting with 'Connection: keep-alive' and followed by a detailed HTTP response header block.

websense®
Content Gateway

User: admin Log Off

Monitor Configure

My Proxy

Basic
Subscription
UI Setup
Snapshots
Logs
Protocols
Content Routing
Security
Subsystems
Networking
SSL

System Access

System Logs

Apply

Log File

content_gateway.out [13.4 KB]

Action

- ☐ Display the selected log file
- ☒ Display last 100 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

Connection: keep-alive

+++++++ Proxy's Response +++++++
-- State Machine Id: 3581
HTTP/1.1 304 Not Modified
Content-Type: application/octet-stream
Last-Modified: Thu, 03 Jan 2013 16:44:02 GMT
ETag: "035789d1e9cd1:0"
Cache-Control: max-age=86400
Date: Mon, 18 Mar 2013 18:51:03 GMT
Age: 0
Proxy-Connection: close
Via: 1.1 MarchWebinar

5. Disable debug logging

The screenshot shows the 'Command Line Utility' window. The 'Module' dropdown is set to 'Websense Content Gateway' and the 'Command' dropdown is set to 'content-line -s'. The 'content-line -s' section is expanded, showing a description: 'Assigns the Content Gateway configuration variable a specified value. See [Content Gateway Help](#) for a list of records.config variables.' The 'Variable Name' field is set to 'proxy.config.diags.debug.enabled' and the 'Value' field is set to '0'. The 'Run' button is highlighted. The 'Console output' pane on the right shows the following text:

```
TS-V5K-GDID1 (Websense Content Gateway)#content-line -s proxy.config.diags.debug.enabled -v 1
content-line -s proxy.config.diags.debug.enabled -v 1

TS-V5K-GDID1 (Websense Content Gateway)#content-line -s proxy.config.diags.debug.tags -v http_hdrs.*
content-line -s proxy.config.diags.debug.tags -v http_hdrs.*

TS-V5K-GDID1 (Websense Content Gateway)#content-line -x
content-line -x

TS-V5K-GDID1 (Websense Content Gateway)#content-line -s proxy.config.diags.debug.enabled -v 0
content-line -s proxy.config.diags.debug.enabled -v 0

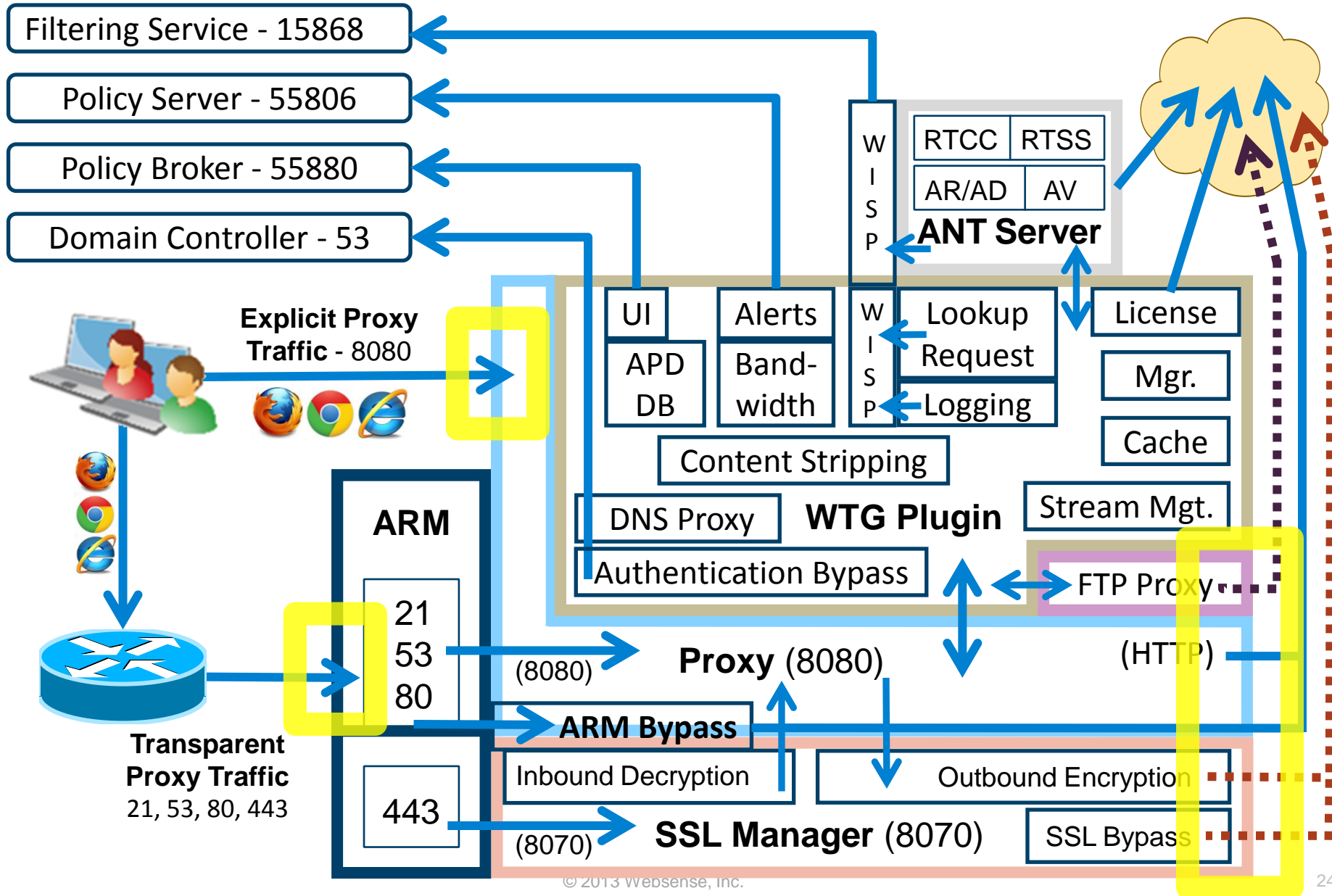
TS-V5K-GDID1 (Websense Content Gateway)#
```

- **Module:** Websense Content Gateway
- **Command:** content-line -s
- **Variable Name:** proxy.config.diags.debug.enabled
- **Value:** 0
- Run

6. Apply changes, run “content_line -x” command

- Enabling debug tag logs
 1. Enable debug logging
 2. Enable one or more debug tags
 3. Reload configuration to apply changes
 4. Reproduce issue and review debugging data
 - In the *content_gateway.out* log
 5. Disable debug logging
 6. Reload configuration to apply changes
- At the command line:
 - If the Content Gateway “bin” directory is not in your path, prepend the `content_line` command with “./” as shown
 - `./content_line -r variable`
 - For multiple tags, use the pipe symbol and exclude extra spaces as shown
 - “`ldap.*|win.*`”
 - For one or more tags, enclose tags with quotes as shown above

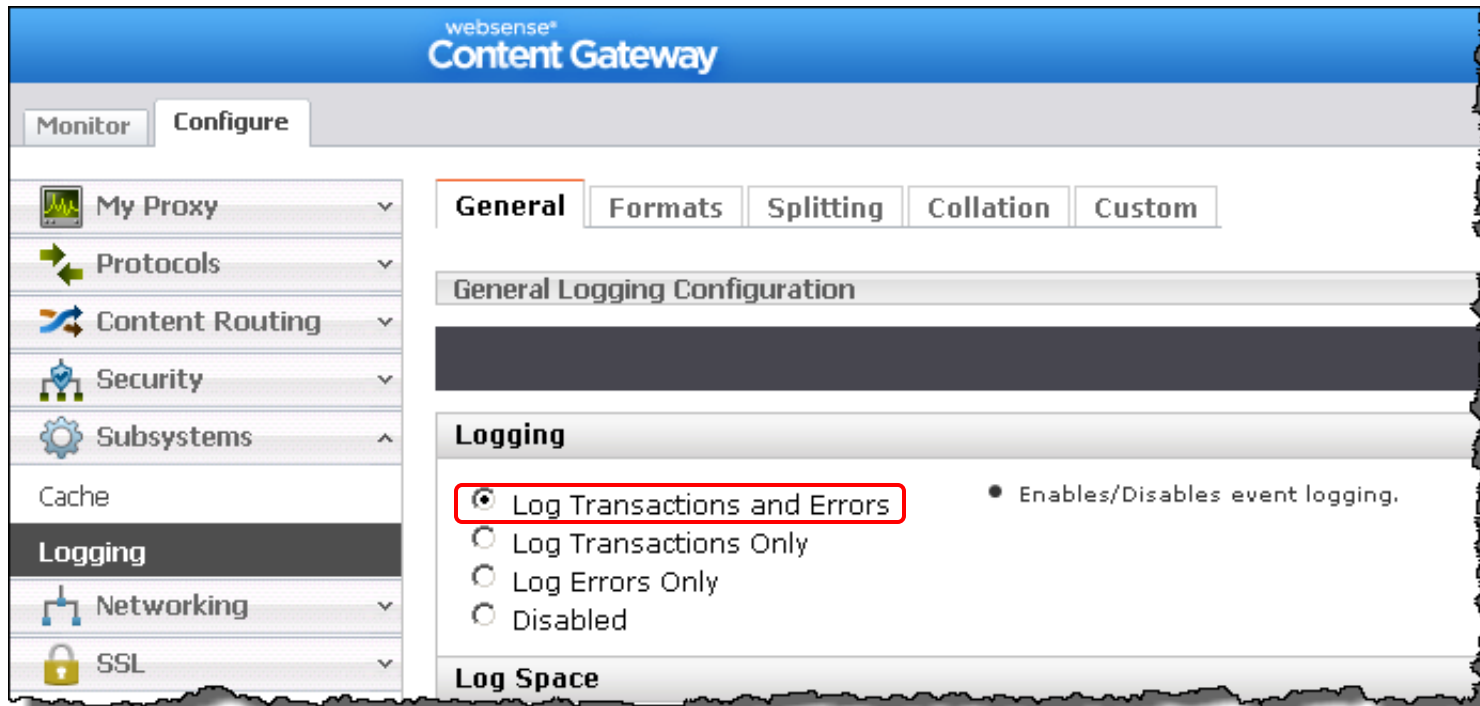
Proxy Access / TCP Connections



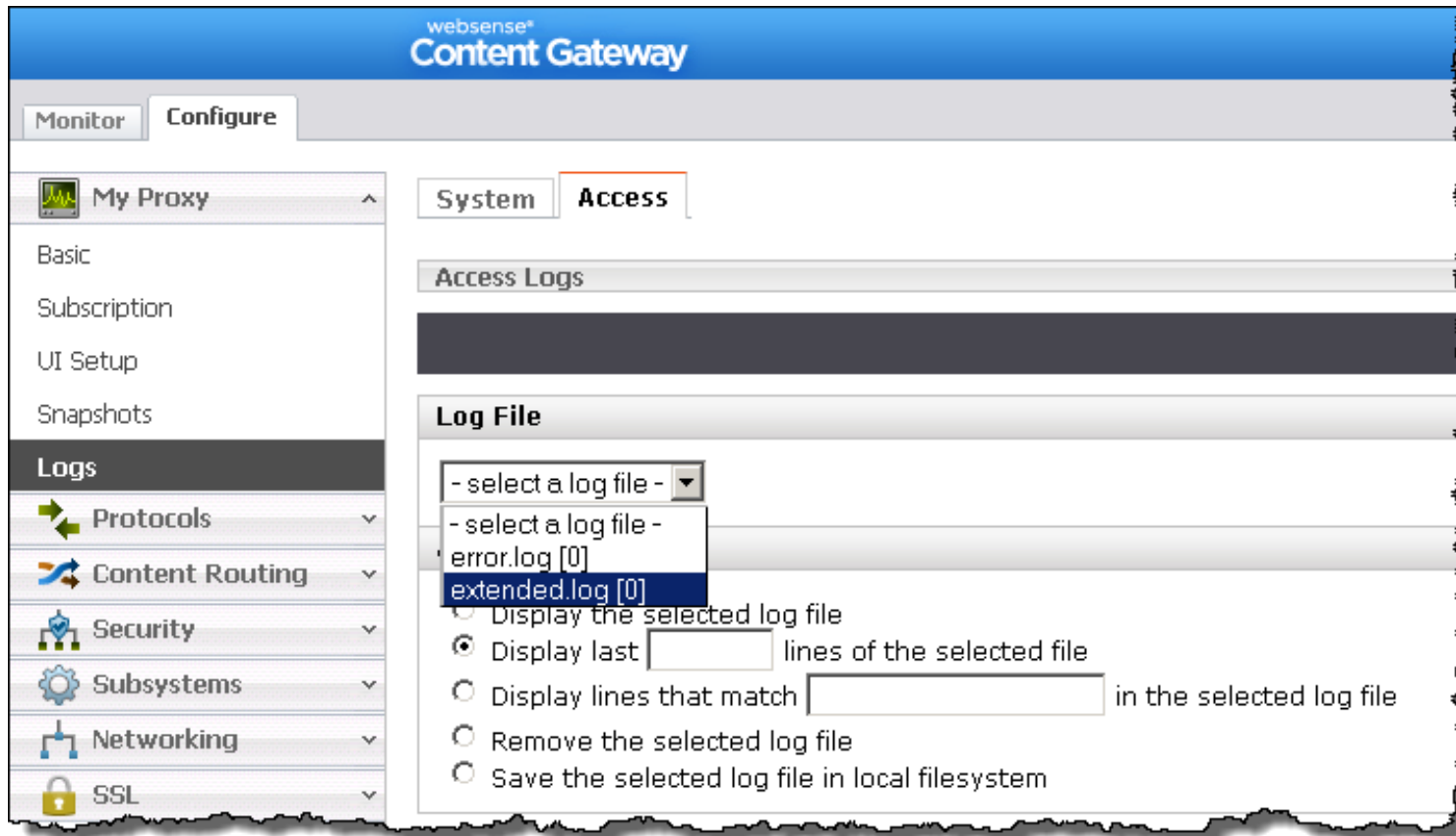
- General proxy access log for TCP connections
 1. Start logging
 - Select Configure > Subsystems > Logging > General tab
 - Select “Log Transactions and Errors” and apply changes
 2. Recreate issue
 3. View logging data
 - Select Configure > My Proxy > Logs > Access tab > Log File > *extended.log* and *error.log*
 - /opt/WCG/logs/extended.log
 - /opt/WCG/logs/error.log
 4. Stop logging when complete
 - Select “Log Errors Only” and apply changes

1. Start logging

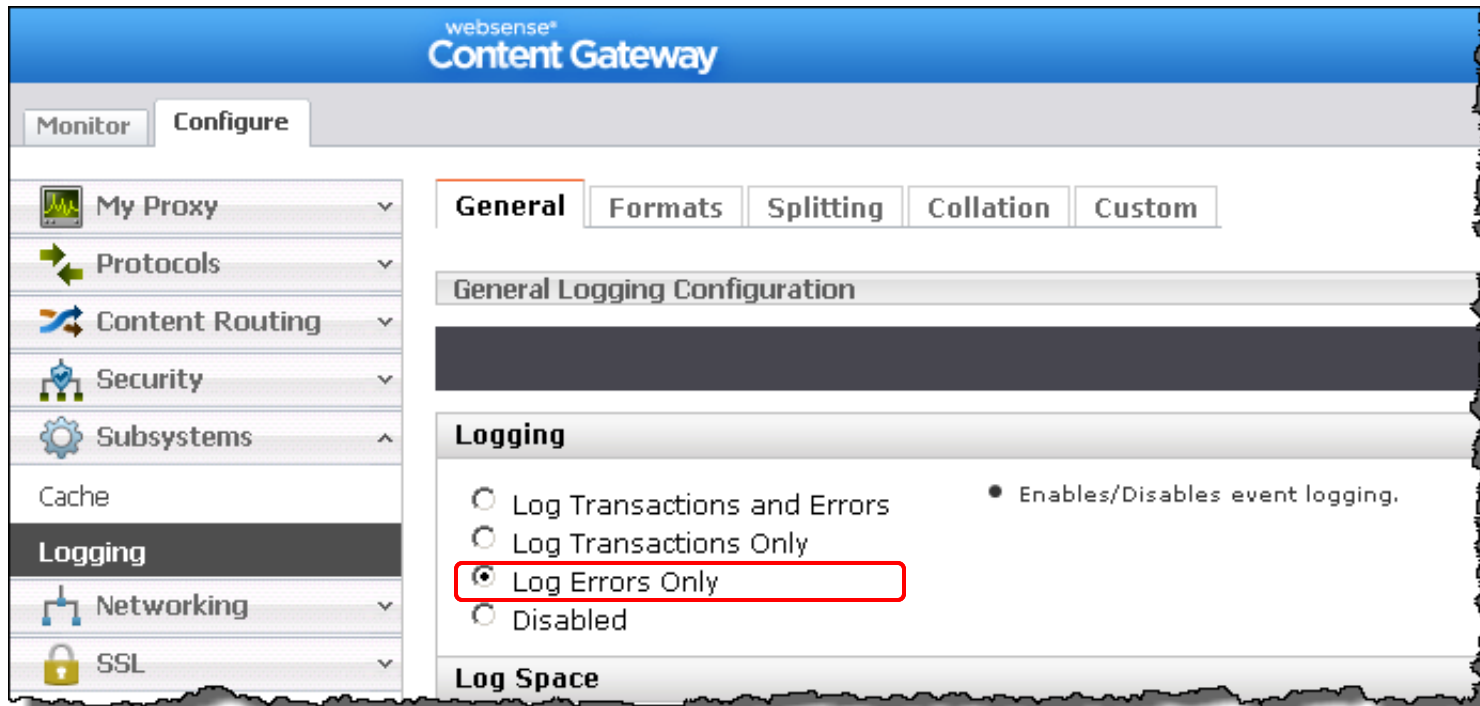
2. Recreate issue



1. Start logging
2. Recreate issue
3. View logging data



1. Start logging
2. Recreate issue
3. View logging data
4. Stop logging



- Content Gateway installed on a Red Hat server
 - `tcpdump -i eth0 -s 0 -w dump.pcap`
- V-Series appliance Command Line Utility

The screenshot shows the 'Command Line Utility' window of a Websense V-Series appliance. The window has a title bar with a question mark and 'Help'. Inside, there's a section titled 'Command Line Utility' with a description: 'The command line utility provides the ability to execute various network debugging commands that are run from any appliance module.'

Below the description, there are two dropdown menus: 'Module:' set to 'Websense Content Gateway' and 'Command:' set to 'tcpdump -w'. To the right of these is a 'Console output:' section with a black background and white text showing the execution of the command. The output includes the command being run, the interface being listened on (eth0), the capture size (65535 bytes), and the results: 17 packets captured, 34 packets received by filter, and 0 packets dropped by kernel.

On the left, under the 'tcpdump -w' command, there's a description: 'Displays information about raw packets from the specified network interface, for packets matching the specified Boolean expression.' Below this, there are two input fields: 'Interface:' set to 'eth0' and 'Expression:' set to 'tcp port 8080'. Both fields have informational icons (i) next to them. At the bottom right of the form are 'Run' and 'Stop' buttons.

Command Line Utility

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

Module: **Websense Content Gateway**

Command: **tcpdump -w**

tcpdump -w

Displays information about raw packets from the specified network interface, for packets matching the specified Boolean expression.

Interface: **eth0**
Only interface(s) associated with selected module are permitted. (i)

Expression: **tcp port 8080**
Filter which packets are displayed (i)

Run **Stop**

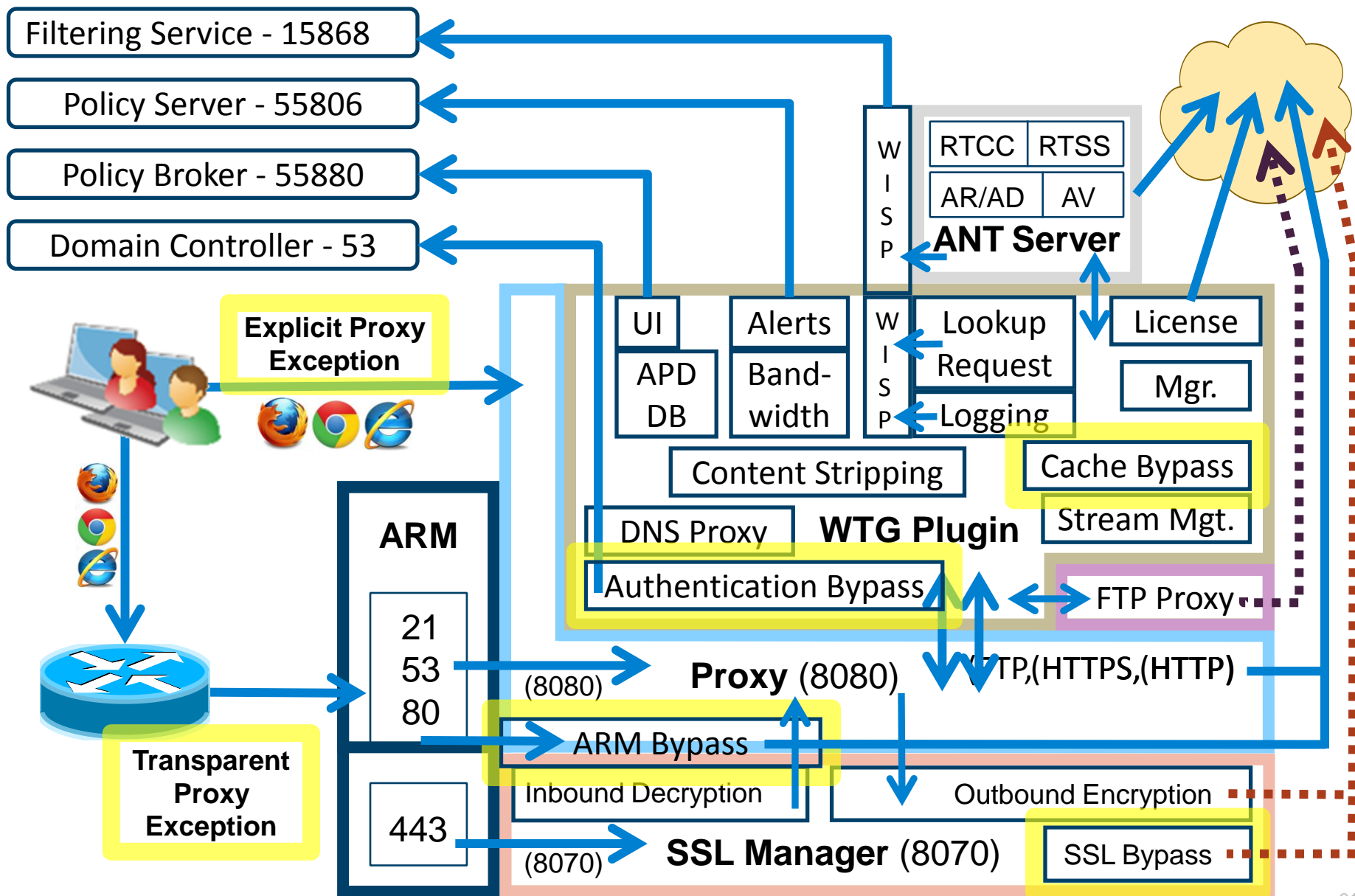
Console output:

```
TS-V5K-GDID1 (Websense Content Gateway)#tcpdump -w output.cap -c 1000  
0 -s 0 -i eth0 -l tcp port 8080  
tcpdump -w output.cap -c 10000 -s 0 -i eth0 -l tcp port 8080  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 b  
ytes  
17 packets captured  
34 packets received by filter  
0 packets dropped by kernel  
  
TS-V5K-GDID1 (Websense Content Gateway)#
```

- Demonstration

- Logs
 - `/var/log/messages`
 - Operating System log and a good place to start looking
 - Contains SSL logging data when syslog is enabled
 - `/opt/WCG/logs/content_gateway.out`
 - Contains debug tag logging data
 - `/opt/WCG/logs/extended.log`
 - Primary log for displaying proxy access events
 - `/opt/WCG/logs/error.log`
 - Primary log for displaying proxy access errors
- Content Gateway management console
 - Configure > My Proxy > Logs > System tab > Log File
 - `messages` and `content_gateway.out`
 - Configure > My Proxy > Logs > Access tab > Log File
 - `error.log` and `extended.log`

Exception, Bypass And Tunnel



- Explicit proxy
 - Add browser exceptions via WPAD, PAC file, GPO or manually
- Transparent proxy
 - Add ACL exceptions to Policy-based routing (PBR), WCCPv2 enabled router or Layer 4 switch
- ARM (transparent proxy only)
 - Add a static bypass rule
- Authentication bypass
 - Edit the filter.config file
- Cache
 - Edit the cache.config file

- Certificate Verification Engine (CVE)
 - Tunnel incidents
- Tunneling
 - Ports
 - Skype
 - Unknown Protocols
- Web Security management console
 - Scanning Options
 - Scanning Exceptions
 - SSL Decryption Bypass
 - Selectively omits sites from decryption
- Demonstration

- This Webinar focused on clarifying the various resources available within the Content Gateway
- This Webinar builds upon the Content Gateway troubleshooting information presented in a previous Webinar titled:
 - [Web Security Gateway - What to do when a Web site does not load as expected](#)
- Please view this prior Webinar. I guarantee you will find it valuable in regards to troubleshooting Websense Content Proxy.

- [Webinar: Web Security Gateway - What to do when a Web site does not load as expected](#)
- [Web sites that have difficulty transiting Content Gateway](#)
- [How to run a packet capture on Websense Content Gateway](#)
- [SSL Manager Certificate Verification Engine v7.7](#)

Webinar Update

Title:

**Quick Start 5: Introducing and configuring Websense®
Cloud Web Security solution**

Date:

April 17, 2013

Time:

8:30 A.M. PST (GMT -8)

How to register:

<http://www.websense.com/content/SupportWebinars.aspx>

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

WebSense Customer Training

Designed for:

- ▶ System administrators
- ▶ Network engineers
- ▶ Other members of your organization as appropriate

Training locations:

All training is conducted at Authorized Training Centers (ATCs). Each ATC has information on costs, course schedules, and types of classes (in-person, virtual, or computer-based).