

#### Websense Web Security Gateway: What to do when a Web site does not load as expected

Websense Support Webinar November 2011

#### **Support Webinars**

010111010

201010101011101010

110010011010101

0101010111010100

# **Webinar Presenter**





#### Title: Technical Support Specialist

- Accomplishments:
  - Over 2 years supporting Websense products

#### Education / Certifications:

- B.Sc (Hons) Computing and IT
- CCNA
- WCWSA Websense Certified Web Security Associate

#### Mike Jones

# **Goals and Objectives**



- Understand how Content Gateway processes a Web request
- Understand how HTTPS packets are processed differently than HTTP packets
- Understand the format of 'extended.log' and 'error.log', and understand how to analyze them
- Understand how to use Wireshark and Fiddler2 to debug a Web site
- Explore common issues

# **Introduction to Content Gateway**



- Content Gateway provides a Web proxy and security gateway for Internet traffic
- Filters Web pages according to Websense Web security policies
- Provides the ability to decrypt SSL connections to inspect contents
- Incorporates real-time content categorization and security scanning
- Can perform transparent or explicit user authentication
- Can cache Web pages to reduce bandwidth usage



#### How an HTTP request is processed by Content Gateway

- 1. WCG receives an HTTP request from the client
- 2. User authentication is performed if configured
- 3. Filtering Service receives the request
- 4. The URL category is determined
- 5. User Service is queried for Active Directory user / group information
- 6. WCG performs real-time content categorization and security scanning as configured
- 7. The Web page is delivered to the client if permitted and safe



#### How an HTTPS request is processed by Content Gateway

- 1. WCG receives an HTTPS request from the client
- 2. User authentication is performed if configured
- 3. If WCG SSL tunnel incident is present, the request bypasses decryption
- 4. The URL category is determined, SSL Category Bypass is checked
- 5. HTTPS is decrypted if required
- 6. Filtering Service receives the request
- 7. User Service is queried for Active Directory user / group information
- 8. WCG performs real-time content categorization and security scanning as configured
- 9. The Web page is delivered to the client if permitted and safe



#### Extended.log

- How to read it
- HTTP response codes and their meaning

#### Error.log

- Failed requests are stored here



## Real-Time Monitor

#### Wireshark

GUI based packet capture

## TCPDump

Linux command line packet capture

## Fiddler2

- How it works
- Diagnosing a problem



#### How to enable

- Go to Configure -> Subsystems -> Logging
- Log files are rotated every 6 hours by default
- Old files are auto-deleted



# Logging Log Transactions and Errors Log Transactions Only Log Errors Only Disabled

# Log Files – Extended / Error.log



#### Viewing Extended.log and Error.log

#### — Go to Configure -> My Proxy -> Logs

	a system	
- My Proxy	Access Logs	
Basic		
Subscription	Log File	
🗖 UI Setup		
Snapshots	- select a log file - 🛛 🔽	
🗖 Logs	- select a log file - error log (644.0 KB)	
+ Protocols	extended.log [8.3 KB]	
Content Routing	Display the selected log file	
+ Security	Oisplay last lines of the selected file	_
+ Subsystems	O Display lines that match	in the selected log file
Networking	Remove the selected log file	
+ SSL	Save the selected log file in local filesystem	

# **Understanding Extended.log**



#### Extended.log field descriptions:



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 Manager online Help by searching for "Netscape Examples"

# **Understanding Extended.log**



#### Extended.log examples

All Extended.log entries contain the source IP, username (if available), date and time the entry was written:

10.0.0.1 - Admin - [01/Oct/2011:11:51:07 -0000]

The rest of the log line shows information about the HTTP(S) request and response Successful HTTP GET request:

"GET http://www.cnn.com/ 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

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



#### Extended.log examples

#### **HTTPS CONNECT request:**

10.5.146.49 - Administrator [31/Oct/2011:14:25:26 -0000] "CONNECT www.cia.gov:443/ HTTP/1.0" 200 39198 200 39198 683 683 564 144 362 0 10

#### Successful HTTP GET request, Web page served from the proxy cache:

10.0.0.1 - - [06/Jul/2010:11:51:07 -0000] "GET http://www.google.com/ HTTP/1.0" **200 64384 304 0** 0 0 204 250 233 222 0

Successful HTTP GET request, Web page served from the client browser cache:

10.0.0.1 - - [06/Jul/2010:11:51:07 -0000] "GET http://www.google.com/ HTTP/1.0" **304 0 304 0** 0 0 204 250 233 222 0

#### **Unsuccessful HTTP GET request:**

10.0.0.1 - - [06/Jul/2010:11:51:07 -0000] "GET http://www.google.com/ HTTP/1.0" 000 0 000 0 0 0 204 250 233 222 **60** 



Extended.log examples

Websense Block message:

"GET http://www.playboy.com/ HTTP/1.0" 302 0 000 0 0 0 133 187 0 0 0 "GET http://10.0.0.20 1:15871/cgi-bin/blockpage.cgi?wssession=687865857 HTTP/1.0" 200 1505 200 1505 0 0 141 144 170 118 0

# **Understanding Error.log**



- When an HTTP(S) request fails it is printed to error.log
- Error.log examples

20110331.07h27m06s RESPONSE: sent 10.5.23.32 status 504 (Unknown Host) for 'sip.websense.com:443/'

20110331.08h16m50s RESPONSE: sent 10.5.146.47 status 502 (NTLM Authentication Failure) for 'http://www.msn.com/'

20110512.08h06m50s RESPONSE: sent 10.5.23.35 status 502 (Windows Authentication Failure) for '216.115.210.210:443/'

20110913.15h55m48s RESPONSE: sent 10.5.22.37 status 502 (Tunnel Connection Failed) for 'websense.com:443/'

## **Debugging Tools – Real-Time Monitor**



- Feature available in v7.6 TRITON Web Security manager
- Scrolling list of URLs processed by Websense
- Shows URLs, user, category, and disposition of URLs
- Can be filtered by these criteria

Real-Time Monitor	- 10.5.144.208				
👌 Customize 🛛				F	ull Screen
Start Pause	Status: Running		Clear Search Filter	s Show	Results
Filter results by:		-			
					A
User ¢	URL ¢	÷	Category 🗢	Action +	Time 👻
administrator	http://by2msg4020516.gateway.m - 672310622.1297131587		Productivity : Instant Messaging	Permitted	16:21:26
administrator	http://www.888.com/		Gambling	Blocked	16:21:26
administrator	http://clients1.google.co.uk/generate_204		Information Technology : Search Engines and Portals	Permitted	16:21:26
administrator	http://www.google.co.uk/		Information Technology : Search Engines and Portals	Permitted	16:21:21
administrator	http://emp.bbci.co.uk/emp/bump?emp=worldwide		News and Media	Permitted	16:21:16
administrator	http://news.bbc.co.uk/sport		Sports	Permitted	16:21:16
administrator	http://www.bbc.co.uk/sport		Sports	Permitted	16:21:11
administrator	http://bbc.co.uk/sport		Sports	Permitted	16:21:11

## **Debugging Tools – Real-Time Monitor**



# Live Demo

Real-Time Monitor	r - 10.5.144.208				_
💫 Customize 🗌				F	ull Screen
Start Pause	Status: Running		Clear Search Filter	rs Show	Results
Filter results by:		1			
					AM
User ¢	URL ¢	ŧ	Category 🗢	Action ¢	Time 🗸
administrator	http://by2msg4020516.gateway.m - 672310622.1297131587		Productivity : Instant Messaging	Permitted	16:21:26
administrator	http://www.888.com/		Gambling	Blocked	16:21:26
administrator	http://clients1.google.co.uk/generate_204		Information Technology : Search Engines and Portals	Permitted	16:21:26
administrator	http://www.google.co.uk/		Information Technology : Search Engines and Portals	Permitted	16:21:21
administrator	http://emp.bbci.co.uk/emp/bump?emp=worldwide		News and Media	Permitted	16:21:16
administrator	http://news.bbc.co.uk/sport		Sports	Permitted	16:21:16
administrator	http://www.bbc.co.uk/sport		Sports	Permitted	16:21:11
administrator	http://bbc.co.uk/sport		Sports	Permitted	16:21:11



- Available for free download at <u>http://www.fiddler2.com</u>
- Creates a 'virtual proxy' on the client
- All HTTP(S) requests and responses that pass through the 'virtual proxy' are shown in different formats
- Has the ability to decrypt HTTPS traffic
  - Inspects the HTTP requests within the HTTPS stream
  - Very useful for debugging problem HTTPS sites
  - Requires installation of Fiddler certificate on the client





<b>Fide</b>	ller - HTT	'P Debuggi	ng Proxy						
<u>File</u>	dit <u>R</u> ules	: <u>T</u> ools ⊻i	ew <u>H</u> elp <u>\$</u> Donate						
Q 49	Replay	🗙 🔹 🕨 Res	sume 🛛 💺 Stream 🇱 🛛	ecode Keep: All sessions 👻	🕀 Any P	rocess 🌺	Find 🔣 Save 🛛	🗓 🏉 Bro	wse 🙀 Clear Cache 🔆 TextWizard 🛛 🔚 Tearoff 🗍 MSDN Search 🛛 👩 🖪 Online 🗙
				Web <u>S</u> essions				<<	🖉 Bequert Builder 🔲 Eilterr 🗍 🗐 Log 🗍 💳 Timeline
#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process 🔺	Challebra Villager Log Auto-Deservedur
5 114	302	HTTP	metrics.turner.com	/b/ss/cnn-adbp-intl/1/H.2	0	no-cac	text/plain	iexplor.	
<b>A</b> 115	5 304	HTTP	i.cdn.turner.com	/cnn/.element/js/3.0/hpse	0	max-ag		iexplor.	Headers TextView WebForms HexView Auth Cookies Raw
🧕 11e	5 200	HTTP	ads.cnn.com	/html.ng/site=cnn_interna	7,202	max-ag	text/html	iexplor.	XML JSON
🔊 117	200	HTTP	ads.cnn.com	/js.ng/site=cnn_internatio	166	max-ag	application/	iexplor.	Request Headers [Raw] [Header Definitions]
5 118	302	HTTP	ads.cnn.com	/event.ng/Type=count&C	0	no-cac	text/html	iexplor.	GET /.element/ssi/misc/3.0/editionvars.html?csilD=csi2 HTTP/1.1
2 119	200	HTTP	i.cdn.turner.com	/cnn/cnnintl_adspaces/2	40,231	max-ag	application/	iexplor.	⊡-Client ▲
5 120	) 302	HTTP	ads.cnn.com	/event.ng/Type=count&C	0	no-cac	text/html	iexplor.	Accept: text/javascript, text/html, application/xml, text/xml, */*
121 🚺	. 200	HTTP	i.cdn.turner.com	/cnn/cnnintl_adspaces/2	17,490	max-ag	application/	iexplor.	Accept-Encoding: gzip, deflate
122 🚺	200	HTTP	b.scorecardresearc	/r?c2=6035748&d.c=gif&	43	private	image/gif	iexplor.	Accept-Language: en-gb
Sec. 23 (123)	3 200	HTTP	www.ugdturner.com	/xd.sjs	341	no-cac	text/javasc	iexplor.	UA-CPU: x86
124	ł 200	HTTP	gdyn.cnn.com	/1.1/1.gif?1320072658811	43	max-ag	image/gif	iexplor.	
Sec. 125	5 200	HTTP	ads.cnn.com	/DartRichMedia_1_03.js	762	max-ag	application/	iexplor.	🕀 Cookies / Login
126	5 200	HTTP	i.cdn.turner.com	/cnn/cnnintl_adspaces/2	16,482	max-ag	application/	iexplor.	
5 127	302	HTTP	ads.cnn.com	/event.ng/Type=count&C	0	no-cac	text/html	iexplor.	adDEmas=R08&broadband&websense.com&0&gbr&826027&0&10198&-&-&-&1
128	3 200	HTTP	edition.cnn.com	/favicon.ico	11,502	max-ag	image/x-icon	iexplor.	
129	200	HTTP	edition.cnn.com	/.element/ssi/www/breaki	255	max-ag	text/html	iexplor.	
S 130	) 200	HTTP	connect.facebook.net	/en_US/all.js	45,063	public,	application/	iexplor.	-s cc=true
131	. 304	HTTP	i.cdn.turner.com	/cnn/.element/img/3.0/pe	0	max-ag		iexplor.	
<b>1</b> 32	2 304	HTTP	i.cdn.turner.com	/cnn/.element/img/3.0/pe	0	max-ag		iexplor.	
133	304	HTTP	i.cdn.turner.com	/cnn/.element/img/3.0/pe	0	max-ag		iexplor.	
134	304	HTTP	i.cdn.turner.com	/cnn/.element/img/3.0/pe	0	max-ag		iexplor.	
<b>\$</b> 135	5 304	HTTP	i.cdn.turner.com	/cnn/.element/img/3.0/pe	0	max-ag		iexplor.	
136	5 200	HTTP	edition.cnn.com	/cnnintl_adspaces/3.0/ho	328	max-ag	text/plain	iexplor.	Response is encoded and may need to be decoded before inspection. Click here to transfo
137	200	HTTP	edition.cnn.com	/.element/ssi/misc/3.0/edi	3,676	max-ag	text/html	iexplor.	Get SyntaxView Transformer Headers TextView ImageView HexView
138	3 200	HTTP	svcs.cnn.com	/weather/getForecast?tim	1,342	max-ag	text/html	iexplor.	WebView Auth Carbing Cookies Daw YMI 150N
139	200	HTTP	connect.facebook.net	/rsrc.php/v1/yK/r/RIxWoz	3,289	public,	application(	iexplor.	
140	) 200	HIIP	i.cdn.turner.com	/cnn/.element/img/3.U/glo	679	max-ag	image/png	lexplor.	The SyntaxView Inspector displays syntax-highlighted html.
141	. 200	HIIP	ads.cnn.com	/html.ng/site=cnn_interna	3,331	max-ag	text/html	lexplor.	script, css, and xml. If you're a web developer, you'll want this add
142	2 302	HTTP	www.racebook.com	/extern/login_status.pnp?	U		text/ntml; c	iexplor.	
143	302	HIIP	www.racebook.com	/extern/login_status.pnp?	0		text/ntmi; c	iexpior.	Download and Install SyntaxView now
144	F 200	HTTP	i.cdn.turner.com	/cnn/.eiement/img/3.u/gio	387	max-ag	image/jpeg	iexpior.	Learn more about SyntaxView and other Inspector add-ons
<b>W</b> 145	304	HTTP	I.can.turner.com	/cnn/cnninti_adspaces/2	0	max-ag	have the line of	iexpior.	Perrove this page
146	302	HIIP	ads.cnn.com	/event.ng/Type=count&c	1 005	no-cac	text/ntmi	iexpior.	
147	200	HTTP	static.ak.rbcdn.net	/connect/xa_proxy.pnp?v	1,305	public,	text/html; c	iexpior.	
	200		static.ak.rbcun.net	/connect/xa_proxy.pnp?v	1,305	public,	text/num; c	iexplor.	
	, 304		i eda turaer com	Icon Lebeneric (Syster)	0	max-ay		iexplor,	
150	, 304 . <b>200</b>	HTTP	edition.cnn.com	l.element/ssi/auto/3.0/se	852	max-ag	text/html	iexplor.	
ALT+O	> type HE	LP							
¦iii∦ ¦iii∦ Rap	turing	= All Proce	esses 1 / 15	1 http://edition.cnn.com/.e	element/ssi	/misc/3.0/e	ditionvars.html?cs	iID=csi2	

----

TTTO

# Fiddler2 – Enabling HTTPS Decryption



- Open Fiddler2, click Tools then Fiddler Options
- Click the HTTPS tab and then the "Decrypt HTTPS" box
- Click Yes to install the Fiddler certificate

Fiddle	er - HTTP	Debugging Proxy	Fiddler Options
ile <u>E</u> di	it <u>R</u> ules	<u>T</u> ools <u>V</u> iew <u>H</u> elp <b></b> ⊈Donate	General HTTPS Extensions Connections Appearance
) <del>4</del> + F	Replay 🗙	Fiddler Options	Fiddler is able to decrypt HTTPS sessions by re-signing traffic using a self-generated certificate.
g . x .		WinINET Options	Capture HTTPS CONNECTs
<u>+</u>	Result	Chara WerthIET Carbo - Chula Chifu M	Fiddler generates a unique root CA certificate to intercept HTTPS traffic.
121	200	Clear WinINET Cookies	Tou may choose to have Windows trust this root certificate to avoid Ignore server certificate errors ONLY click 'Yes' on a computer used exclusively for TEST purposes.
122 123	200 200	Text Encode/Decode Ctrl+E	Skip decryption for the following hos You should click 'No' unless you're very very sure.
124	200	Compare bessions	
125	200	Reset Script	Trust the Fiddler Root certificate?
126 127 128 128	200 302 200 200	<u>S</u> andbox <u>V</u> iew IE Cache <u>H</u> OSTS	Export Fiddler Root Certificate to Desktop Remove Interception Certificates
-			Help         Note: Changes may not take effect until Fiddler is restarted.         OK         Cancel

# Fiddler2 – Enabling HTTPS Decryption



# Live Demo

er - HTTP	Debugging Proxy
it <u>R</u> ules	<u>T</u> ools <u>V</u> iew <u>H</u> elp <u>\$</u> Donate
Replay 🄀	<u>F</u> iddler Options
	WinINET Options
Result	Clear WinINET Cache Ctrl+Shift+X
200	– Clear WinINET Cookies
200	
200	Text <u>E</u> ncode/Decode Ctrl+E
200	Compare Sessions
200	Reset Script
200	
302	<u>S</u> andbox
200	⊻iew IE Cache
200	HOSTS
	er - HTTP t <u>R</u> ules Replay X Result 200 200 200 200 200 200 200 20

Fiddler Options	×
General HTTPS Extensions Connections	Appearance
Fiddler is able to decrypt HTTPS sessions by re	e-signing traffic using a self-generated certificate.
Capture HTTPS CONNECTS	NING: Sharp Edges! Read Carefully!
☑ Decrypt HTTPS traffic	Fiddler generates a unique root CA certificate to intercept HTTPS traffic. You may choose to have Windows trust this root certificate to avoid
	ONLY click 'Yes' on a computer used exclusively for TEST purposes.
Skip decryption for the following hos	You should click 'No' unless you're very very sure.
	Trust the Fiddler Root certificate? Yes
Export Fiddler Root Certificate to Desk	top <u>R</u> emove Interception Certificates
Help Note: Changes may not take effect of	until Fiddler is restarted. <u>QK</u> <u>Cancel</u>

# **Wireshark - Introduction**



- Available for free download from <a href="http://www.wireshark.org">http://www.wireshark.org</a>
- Captures TCP packets from the network interface
- Captures can be filtered by protocol, IP address, TCP port, and many other criteria



# Wireshark – How to Capture



- Click the 'Start Capture' button and choose a network interface
- Perform the test you want to capture
- Use filters to display the information you require
  - Click the button below



Select your capture interface



# Wireshark – Example Capture



- Capture showing a connection to <u>www.google.co.uk</u> through a proxy
- Using display filter "HTTP"
- Shows packet #, Time, Source and Destination IPs, Protocol, and Info

_					
📶 (Untitle	d) - Wireshark				
<u>E</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u>	nalyze <u>S</u> tatistics Tele	phon <u>y I</u> ools <u>H</u> elp		
	ok (m)   E (	<b>. x 2</b> 4   °	् 🗢 🗢 🖓 🔂		O, Q, Q, 🗹   🎬 🗹 畅 💥   💢
Filter: http	)		▼ Expr	ession Cle	ar_Apply
No. +	Time	Source	Destination	Protocol	Info
106	4.308400	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/ HTTP/1.1
126	4.370361	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (text/html)
144	4.782315	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/close_sm.gif HTTP/1.1
149	4.793138	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/icons/product/chrome-
154	5.260968	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
156	5.399601	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (GIF89a)
161	5.813632	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-bg
163	5.815601	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-lo
168	5.818564	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/mgyhp_sm.png HTTP/1.1
173	5.821863	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/srpr/nav_logo80.png H
178	5.836095	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/modules/buttons/g-but
184	5.838423	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/modules/buttons/g-but
187	5.838566	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-pl
193	5.839962	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-c.
195	5.854529	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
231	5.886029	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
241	5.897502	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (GIF89a)
245	5.900820	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (GIF89a)
299	5.905084	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
312	5.906028	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
340	5.917829	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)

# Wireshark



25

TTO

# Live Demo

711-1-1-1-1	dX tubo de ente				
	ed) - wiresnark				
<u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u>	<u>Analyze Statistics Tele</u>	phon <u>y T</u> ools <u>H</u> elp		
8		<b>. x 2</b> 占   °	् 🗢 🗢 🖓 🔂 🕹		⊕, ⊖, ⊕,    🕍 🍢 🎋   🧝
Filter: ht	τp		▼ E <u>x</u> pr	ession Cle	a <u>r</u> App <u>l</u> y
No	Time	Source	Destination	Protocol	Info
10	5 4.308400	10.5.146.45	10.5.144.170	HTTP	GET http://www.qooqle.co.uk/ HTTP/1.1
12	5 4.370361	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (text/html)
144	4.782315	10.5.146.45	10.5.144.170	HTTP	<pre>GET http://www.google.co.uk/images/close_sm.gif HTTP/1.1</pre>
14	9 4.793138	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/icons/product/chrome-
154	4 5.260968	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
15	5 5.399601	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (GIF89a)
16	L 5.813632	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-bg
16	3 5.815601	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-lo
16	3 5.818564	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/mgyhp_sm.png HTTP/1.1
17	3 5.821863	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/srpr/nav_logo80.png H
17	3 5.836095	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/modules/buttons/g-but
184	4 5.838423	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/images/modules/buttons/g-but
18	7 5.838566	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-pl
19	3 5.839962	10.5.146.45	10.5.144.170	HTTP	GET http://www.google.co.uk/logos/2011/halloween11-hp-c.
19	5 5.854529	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
23:	L 5.886029	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
24:	L 5.897502	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (GIF89a)
24	5 5.900820	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (GIF89a)
29	9 5.905084	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
31.	2 5.906028	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)
34)	0 5.917829	10.5.144.170	10.5.146.45	HTTP	HTTP/1.1 200 OK (PNG)



# Wireshark – Useful Display Filters

#### Filter by protocol

- HTTP / DNS / FTP / SMB etc.
- Filter by IP address
  - Ip.addr == 10.1.1.1
- Filter by TCP port
  - Tcp.port == 8080
- Filter by TCP flags
  - Tcp.flags.reset == 1
  - Tcp.flags.syn == 1

#### Combine any number of different filters using 'and' (&&), 'or' (||) and 'not' (!) conditions

– Ip.addr == 10.1.1.1 || ip.addr == 10.2.2.2 && tcp.port == 8080



#### Basic tcpdump command

- tcpdump –np –s 0 –i any –w output.pcap
- -np = non-promiscuous
- -i any = capture all network interfaces, can use '-i eth0' if required

#### Using tcpdump input filters

- Similar to Wireshark, except filtered packets are not saved to the capture
- Filters: 'host', 'port' and 'icmp' can be used

If you do not specify the –w switch tcpdump output is sent to the console

- Not very user friendly, but useful for testing basic connectivity between devices
- TCPDump example input filter usage
  - host 10.1.1.1 or host 10.2.2.2 and port 8080
  - host 10.1.1.1 or host 10.2.2.2 or port 53 or icmp
- Can be run from the Command Line Utility in the Appliance Manager

# **TCPDump**



29

#### TCPDump on the command line – same HTTP request for www.google.co.uk as in the Wireshark capture

root@xyz logs]# tcpdump -np -s O -i any port 8080 -nn	
cpdump: verbose output suppressed, use -v or -vv for full protocol decode	
istening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes	
6:04:05.606572 IP 10.5.146.45.1904 > 10.5.144.170.8080: S 294789217:294789217(0) win 64240 <mss 1460,nop<="" td=""><td>, n</td></mss>	, n
6:04:05.606658 IP 10.5.144.170.8080 > 10.5.146.45.1904: S 1320037730:1320037730(0) ack 294789218 win 584	0
6:04:05.609528 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 1 win 64240	
6:04:05.609692 IP 10.5.146.45.1904 > 10.5.144.170.8080: P 1:607(606) ack 1 win 64240	
6:04:05.609705 IP 10.5.144.170.8080 > 10.5.146.45.1904: . ack 607 win 6666	
6:04:05.663341 IP 10.5.144.170.8080 > 10.5.146.45.1904: P 1:275(274) ack 607 win 6666	
6:04:05.675337 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 275:1707(1432) ack 607 win 6666	
6:04:05.675721 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 1707 win 64240	
6:04:05.675730 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 1707:6003(4296) ack 607 win 6666	
6:04:05.676121 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 4571 win 64240	
6:04:05.676129 IP 10.5.144.170.8080 > 10.5.146.45.1904: . $6003:10299(4296)$ ack 607 win 6666	
6:04:05.676420 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 7435 win 64240	
6:04:05.676428 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 10299:14595(4296) ack 607 win 6666	
6:04:05.676669 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 10299 win 64240	
6:04:05.676677 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 14595:16027(1432) ack 607 win 6666	

# **TCPDump**



## Live Demo

[root@xyz logs]# tcpdump -np -s 0 -i any port 8080 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
16:04:05.606572 IP 10.5.146.45.1904 > 10.5.144.170.8080: S 294789217:294789217(0) win 64240 <mss 1460,nop,<="" td=""></mss>
16:04:05.606658 IP 10.5.144.170.8080 > 10.5.146.45.1904: S 1320037730:1320037730(0) ack 294789218 win 5840
16:04:05.609528 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 1 win 64240
16:04:05.609692 IP 10.5.146.45.1904 > 10.5.144.170.8080: P 1:607(606) ack 1 win 64240
16:04:05.609705 IP 10.5.144.170.8080 > 10.5.146.45.1904: . ack 607 win 6666
16:04:05.663341 IP 10.5.144.170.8080 > 10.5.146.45.1904: P 1:275(274) ack 607 win 6666
16:04:05.675337 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 275:1707(1432) ack 607 win 6666
16:04:05.675721 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 1707 win 64240
16:04:05.675730 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 1707:6003(4296) ack 607 win 6666
16:04:05.676121 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 4571 win 64240
16:04:05.676129 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 6003:10299(4296) ack 607 win 6666
16:04:05.676420 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 7435 win 64240
16:04:05.676428 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 10299:14595(4296) ack 607 win 6666
16:04:05.676669 IP 10.5.146.45.1904 > 10.5.144.170.8080: . ack 10299 win 64240
16:04:05.676677 IP 10.5.144.170.8080 > 10.5.146.45.1904: . 14595:16027(1432) ack 607 win 6666

30

21110



Always test a problem Web site direct without the proxy to see if the issue remains

- If the site still does not load correctly direct you should contact the Web site administrators
- Test a Web site using an unrestricted policy
  - Partial blocks can prevent Web sites from displaying correctly
  - If the page loads correctly you need to adjust your policies
- If the Web site is HTTPS, test it using an SSL Tunnel
  - Many HTTPS sites fail if their traffic is decrypted
  - In particular Citrix systems and applications
- If needed, log a support case with Websense
  - Provide log files and debugs with the case to help speed resolution



### 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.

#### <u>ask.websense.com</u>

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



- Search Understanding HTTP Response Codes
  - <u>http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html</u>
- Fiddler2 Help And Tutorials
  - <u>http://www.fiddler2.com/fiddler/help/</u>
- Wireshark Help And Tutorials
  - <u>http://www.wireshark.org/docs/</u>
- Additional Wireshark Display Filters
  - <u>http://wiki.wireshark.org/DisplayFilters</u>



TTTO

	Title: Configuring WCCP v2 with Websense Content Gateway – the web proxy for Web Security Gateway
Webinar	Date: December 14, 2011
Update	Time: 8:30 A.M PDT (GMT -7)
	How to register: http://www.websense.com/content/SupportWebin ars.aspx



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

Authorized Training Partner

Certified Instructor







