

SSL Decryption: Benefits, Configuration and Best Practices

Websense Support Webinar January 2013

TRITONTM

Web security Email security Data security Mobile security

© 2012 Websense, Inc.

Presenter





Matt Bruce

Title:

- Sr. Technical Support Specialist
- Accomplishments:
 - Backline Support
 - Linux and Internet services specialist
 - 8 years supporting security appliances
- Qualifications:
 - 16 years experience
 - ISP and security background

- Why enable SSL decryption?
- Enabling SSL
- SSL Decryption Bypass
- Subordinate CA/self-signed certificates
 - Why should my organisation install a certificate?
 - Installing a Subordinate CA
 - Installing a self-signed Root certificate
- Handling SSL Incidents

Why enable SSL decryption?

- Organisations without SSL decryption typically Allow all or Block all SSL traffic
- SSL decryption improves adherence to organisational policies
 - Access control
 - Monitoring
 - Reporting
- Improves organisational and user security
 - Reduced risk of interception
 - Adds the ability to control hosts and the Categories users can browse
- Clients see Block Page when browsing disallowed hosts
 - Shows reason/Category
 - Increases awareness of organisation policies
 - Can allow access subject to specific criteria (e.g. time, confirmation)
- Comparison of connection logs with and without SSL decryption enabled
 - An extended.log example **without** SSL decryption:

^{10.5.144.32 - [12/}Jan/2013:15:43:51 -0000] "CONNECT www.cia.gov:443/ HTTP/1.0" 200 127 200 0 0 0 383 127 542 76 0

Why enable SSL decryption? (Cont'd)

- An extended.log example with SSL decryption:
- 10.5.144.32 [12/Jan/2013:15:43:51 -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/Jan/2013:15:43:52 -0000] "GET http://www.cia.gov/javascript/register_functioncachekey1018.js HTTP/1.1" 200 52663 200 52663 0 0 840 297 829 287 0
- 10.5.144.32 - [12/Jan/2013:15:43:53 -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/Jan/2013:15:43:53 -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/Jan/2013:15:43:53 -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/Jan/2013:15:43:53 -0000] "GET http://www.cia.gov/javascript/javascript.js HTTP/1.1" 200 6092 200 6092 0 0 820 296 809 286 0

- SSL decryption uses the Man In The Middle (MitM) method
- For more information on the extended.log file format, see:

http://www.websense.com/content/support/library/web/v77/wcg_help/nscape.aspx

- Where to find extended.log file:
 - WCG Manager: Configure > My Proxy > Logs > Access > Log File
 - Software: /opt/WCG/logs/extended.log

Enabling SSL



- Enable the HTTPS protocol in Features
 - Adds new SSL menu to the left

	websense* Content Gateway			User: admin	Log C
Monitor Configure					P He
My Proxy	General Clustering				
Basic			Apply	Cancel	
	Restart				
Snapshots Logs	Restart	 Restarts V manager : 	Vebsense Conter services on all no	nt Gateway prox odes in the clust	y and :er.
Protocols	Proxy Name				
Content Routing Security Subsystems	R. Colling and	 Specifies t Gateway n In a Webs nodes mu 	the name of the ode/cluster. sense Content Ga st share the sam	Websense Cont ateway cluster, a ne name.	ent ill
Networking 🗸 🗸	Alarm Email				
SSL v	KOLON DARAGE CON	 Specifies t Content G 	the email addres ateway will send	s to which Webs alarm notificatio	iense ons.
	Features				
		Feature		On	Off
	Protocols				
	FTP			\odot	۲
	HTTPS			۲	0
1	Networking				

- Allows selective and controlled use of SSL decryption and bypass
- Easy to use exclusion from SSL decryption
- Exclusion options:
 - Category selection similar to Category Filters
 - Privacy Categories: Simple selection of Categories most organisations prefer to bypass
 - Client: Source IP addresses/ranges
 - Destination: Destination hosts, URLs, or IP addresses/ranges
- Demonstration: SSL Decryption Bypass options

SSL Decryption Bypass (Cont'd)

Comparing SSL Decryption Bypass logs
 – Example SSL Bypass by Category:

(wtg_txn_url) [7613] URL: https://www.hsbc.co.uk

(wtg_txn_wisp) [7613] WispClient (tid=59104): Doing http lookup with 0 dynamic

category and 0 TFT, src ip: 10.5.146.50

(wtg_txn) [7613] EIM(Out/Hdr) returned category 68, allowed

(wtg_txn_ssl) IsCategorySSLDecryptBypassed: category=68 matched with: 68

(wtg_txn_ssl) [7613] Bypassing SSL Decryption (not blocked)

(wtg_txn_result) [7613] 10.5.146.50->91.214.6.98 User[] ReqMethod[CONNECT] Category[Financial Data and Services] Disposition[CATEGORY_NOT_BLOCKED] ContentType[] Reason[] DynCat[0] RecBit[0] Bytes[Sent=83 Rcvd=0]

SSL Decryption Bypass (Cont'd)

– Example SSL Bypass by Client IP:

```
(wtg_txn_url) [7625] URL: https://www.hsbc.co.uk
(wtg_txn_wisp) [7625] WispClient (tid=59104): Doing http lookup with 0 dynamic
category and 0 TFT, src ip: 10.5.146.50
```

(wtg_txn) [7625] EIM(Out/Hdr) returned category 68, allowed

(wtg_txn_ssl) **IsClientSSLDecryptBypassed**: srcIP=10.5.146.50 matched with: first= 10.5.146.50 last= 10.5.146.50

(wtg_txn_ssl) [7625] Bypassing SSL Decryption (not blocked)

(wtg_txn_result) [7625] 10.5.146.50->91.214.6.98 User[] ReqMethod[CONNECT]
Category[Financial Data and Services] Disposition[CATEGORY_NOT_BLOCKED]
ContentType[] Reason[] DynCat[0] RecBit[0] Bytes[Sent=83 Rcvd=0]

- Visible in the content_gateway.out log file:
 - WCG Manager: Configure > My Proxy > Logs > System
 - Software: /opt/WCG/logs/content_gateway.out

Why should we install a certificate?

- Enabling SSL decryption gives certificate errors when browsing HTTPS sites
 - Client unable to verify integrity of self-signed certificates
 - Installing a certificate takes care of this
- Allows clients to browse without seeing a certificate warning for every HTTPS host
 - Reduces user confusion and related helpdesk calls
 - Browsing HTTPS host without certificate installed



Why should we install a certificate? (Cont'd) websense

- Browsing HTTPS host with certificate installed



Why should we install a certificate? (Cont'd) websense

• Browser toolbar collector, or "Why is my Internet so slow?"

APIVISION * 🗟 * 🚳 * 🛍 * 📾 * 🛄 🤬 🕸 🖧 * 🍲 C * 🗢 D * 🔮 E * 😤 F * 😤 H * 😤 N * 😤 Z * 🚺 💁 🛛 APIVISION.COI	42
🗿 Microsoft Corporation - Microsoft Internet Explorer	<u>u</u> ×
File Edit View Favorites Tools Help	
🔾 😋 Back + 🕗 - 💌 😰 🚮 🔎 Search 🤺 Favorites 🜒 Media 🊱 🔗 + 🍃 🚍 + 🛄 🍫 💓 🖃 🌮 Folders 🛧 + 🐰 📋 🗊 🗊	»
Address 🙋 http://www.microsoft.com/	50
🔄 Google - 💽 📸 Search Web 😻 Search Site 🛛 🖓 News 🛛 Page Info + 💼 Up 🥒 Highlight	1
Search 🚽 📼 🔹 Sign in 🧐 My Yahoo! 🗸 🦅 HotJobs 👻 Yahoo! 👻 🕜 Shopping 👻 🗗 Games 👻 Yahoo! Mail 🔹 🔗 News 📼	>>
🖉 🕼 🖅 🖉 🖉 Highlight 🔀 Email this page to a friend 🔞 JeevesLin	ks
🖞 👉 DAP 🖞 Options 🔚 Software 🔽 💦 🖓 🛱 D/L 0 files 🕰 🗸 💰 🔹	
AimAtSite 🗾 🛃 History 👰 Favorites 🔊 This Page 🦚 Online + 🎬 Tools +	
VPRAIZE + Web 🔽 Search 🗞 Channels + 🕅 My Praize + 🖂 Praize Mail + 🙎 IM + 💼 Favorites +	
🛛 🚾 MapStannet 🔹 🧰 😨 🧟 Search 🛛 🦧 Discover 🔏 My Plan 🛛 👸 Daily Plan 👔 Best Sites	
Search	Go
📐 Addresses.com Search Type: Email Search 🔻 Name/Business: 🔹 🔽 Locale: 💌 Search 🔞 Search Tips	
Search 🌽 Highlight 🔏 Email this page to a frier	nd
TEOMA Search Image: Highlight Image: Email this page to a frier Microsoft Software Image: Email this page to a frier Search Image: Email this page to a frier Search Search Image: Email this page to a frier Search Image: Email this page to a frier Image: Email this page to a frier Search Image: Email this page to a frier Image: Email this page to a frier	nd
Search Search Highlight Email this page to a frier Microsoft Software Tech News Windows 2000 Internet Search Q (Skins Web v) Ultrabar Google * Image: Search Highlight Search Q (Skins Web v)	nd
Search	nd
Search Search Highlight Email this page to a frier Microsoft Software Tech News Windows 2000 Internet Computer Hardware Search Search <td>nd</td>	nd
Search & Highlight & Email this page to a frier Search & Highlight & Email this page to a frier Microsoft & Software & Tech News & Windows 2000 & Internet & Computer Hardware Search &	nd
Search Search Microsoft Search Mighlight Email this page to a friet Microsoft Software Tech News Windows 2000 Internet Computer Hardware Search Search<	nd
Image: Search in this page to a frie Image: Search in this page	om.
Search S	nd Som

Source: scapegoatmedia.com

Installing a Subordinate CA

- For environments with Microsoft Certificate Server
- Uses existing organisational Root CA
- Basic steps:
 - 1. Use OpenSSL 0.9.8x (Windows or Linux) to create Certificate Signing Request (CSR) and private key

openssl req -new -newkey rsa:2048 -keyout wcg.key -out wcg.csr

- 2. Sign CSR with Microsoft Certificate Services to create and export Subordinate CA
- 3. Import certificate and private key into Content Gateway
- 4. Restart Content Gateway
- Detailed procedure and further information: http://www.websense.com/content/support/library/web/v77/

http://www.websense.com/content/support/library/web/v77/wcg_help/ ssl_sub_ca.aspx

• Windows version of OpenSSL 0.9.8x:

http://www.websense.com/support/article/kbarticle/How-to-use-OpenSSL-and-Microsoft-Certification-Authority

Demonstration: Installing a Sub CA

Installing a self-signed certificate

- For environments without a Certificate Server
- Deployment options
 - Locally on each client via manual import
 - Centrally via AD Trusted Certificate Store
- Steps to install self-signed certificate from Content Gateway to an IE9 client
 - 1. Export Public CA Key from Content Gateway



2. Open exported certificate file to view its details

Certificate	X
General Details Certification Path	
Certificate Information	
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	
Issued to: ts151-vm	
Issued by: ts151-vm	

3. Open Internet Options on client and view installed certificates

Internet Op	tions					B S
General	Security	Privacy	Content	Connections	Programs	Advanced
Content	Advisor					
	Rating: viewed	s help you I on this c	i control the omputer.	e Internet cont	tent that car	1 be
			🕘 📴	able	😗 Se <u>t</u> ti	ngs
Certifica	tes —					
	Use ce	rtificates	for encrypt	ed connections	and identifi	ication.
	llear <u>S</u> SL :	state	<u>C</u> ertif	ficates	Pu <u>b</u> lishe	ers
AutoCom	nplete —					

websense

4. Click Import to start Certificate Import Wizard

(Certificates				X
Intended purpose: <all< td=""><td>></td><td>uthorities Tru</td><td>isted Root Certification</td><td>•</td></all<>	>	uthorities Tru	isted Root Certification	•
Issued To	Issued By	Expiratio	Friendly Name	
	Remove		Adva	
Certificate intended purpos	es			iceu
			View	
Learn more about <u>certificate</u>	2		Clo	se

websense

5. Import the certificate into the "Trusted Root Certification Authorities" certificate store



6. A warning that the root certificate being imported cannot be validated may appear; select Yes to import it



websense

7. Certificate Import Wizard shows a popup on successful completion



8. Verify the certificate is in the correct location

Certificates				X
I <u>n</u> tended purpose:	All> n Authorities Trusted Roo	ot Certification Aut	horities Trusted Pu	
Issued To	Issued By	Expiratio	Friendly Name	*
Thawte Premium So Thawte Premium So Thawte Primary Ro	tempCA Thawte Premium Serv thawte Primary Root i Thawte Timestamping	17/07/2017 31/12/2020 CA 16/07/2036 31/12/2020	<none> thawte thawte Thawte Timesta</none>	
UTN - DATACorp S	ts 151-vm GC UTN - DATACorp SGC	24/06/2019	<none> USERTrust</none>	

Comparison of certificate information



Direct (no proxy)



websense

Self-signed certificate

Certificate Verification Engine (CVE)

- Verifies the integrity of certificates
 - Provides gateway-level ability to perform certificate checks
 - Supplements modern client certificate checks
- Required when SSL decryption is enabled
- Uses revocation lists to maintain current list
- Customisable to allow fine-tuning
 - Individual options can be enabled or disabled as needed
- More information:

http://www.websense.com/content/support/library/web/v77/wc g_ssl_cve/Certificate%20Verification%20Engine%20v77.pdf http://www.websense.com/content/support/library/web/v77/wc g_ssl_cve/cve_options.aspx http://www.websense.com/content/support/library/web/v77/wc g_help/c_valid.aspx

- Incidents automatically generated when client receives an "access denied" message due to:
 - Hosts requiring client certificates
 - Validation via the Certificate Verification Engine (CVE) fails
- Administrators can choose what happens when client visits a site in Incident list:
 - Allow: Client can access website even if certificate is invalid
 - Blacklist: Client cannot access website at all
 - Block: Client cannot access website, unless Verification Bypass is enabled (system presents "Visit site anyway" button on denial page)

Best Practices & Troubleshooting

- Enable Certificate Verification Engine (CVE)
 - Needs to be enabled when SSL decryption is used
 - Provides a layer of certificate checking over entire network
- Enable Verification Bypass if required
 - Lets users to bypass sites automatically-added to SSL Incidents
 - Depends upon organisation's priorities and requirements
- SSL can be configured to use syslog
 - Allows centralised logging for analysis or processing
- Customise, brand or translate SSL error messages
 - "Certificate Failure" and "Connect Error" pages
- Periodically examine the SSL Incident List
 - CVE automatically adds entries to the Incident List
 - Treat like a quarantine mailbox by checking and verifying the entries there.

Best Practices & Troubleshooting (Cont'd)

websense

- Testing Categories with HTTPS using the Websense Master Database Test Pages
 - Test Blocked category or real-time content

https://testdatabasewebsense.com/sex

https://testdatabasewebsense.com/realtime/SexAndAdult.html

Conte	ent blocked by your organization
Reason:	This Websense category is filtered: Sex.
URL:	https://testdatabasewebsense.com/sex

Test Allowed category

https://testdatabasewebsense.com/news

News & Media

This page has been categorized in the Websense Master Database as "News & Media."

If you can access this page, Web pages in this category are **not blocked** for this user or machine.

Best Practices & Troubleshooting (Cont'd)

websense

Test malicious file download (safe):

https://testdatabasewebsense.com/realtime/maliciouswebsites/m alicioustest2.exe

🐼 Secur	ity risk blocked for your protection
Reason:	This Websense category is filtered: Potentially Unwanted Software. Sites in this category may pose a security threat to network resources or private information, and are blocked by your organization.
URL:	http://testdatabasewebsense.com/realtime/maliciouswebsites/malicioustest2.exe

Schowledge 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.

websense

Title:

Quick Start 3: Installing and Configuring Websense Content Gateway

Webinar Update Date:

February 20, 2013

Time: 08:30am PDT (GMT-8)

How to register:

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

websense

Training

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

readiness@websense.com



Questions?





© 2012 Websense, Inc.