



DPI-SSL

Selling, Sizing, Implementing, & Managing DPI-SSL
Presented by Rob Krug

SONICWALL™

AGENDA

- Selling the solution
- Sizing the opportunity
- Implementing a successful deployment
- Management & Troubleshooting

The Threat



Normally, when you try to connect securely, sites will present trusted identity that you are going to the right place. However, this site's identity can't be v

What Should I Do?

If you usually connect to this site without problems, this error could mean t trying to impersonate the site, and you shouldn't continue.

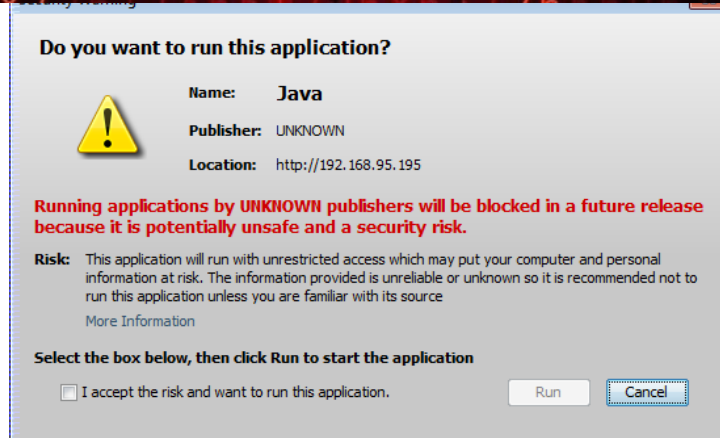
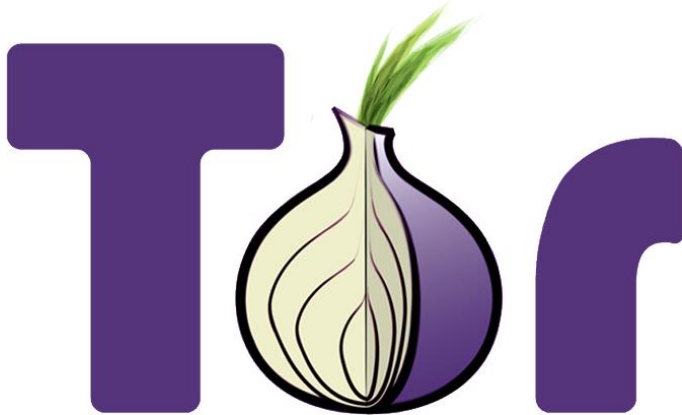
[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**



Your connection is not private

Attackers might be trying to steal your information from **yoursite.com** (password, messages, credit cards etc)





Stateful Packet Inspection

Here the “inspection”, which is an everyday police officer directing traffic, can only see the cars coming into the intersection. From there it can only identify the traffic by the type of car and the direction it is travelling

Deep Packet Inspection

In Deep Packet Inspection, our police officer becomes Superman with x-ray vision, and can now see inside the cars as they come into the intersection. He can see the driver, what is in the trunk, see what is under the hood, and the determine to let the traffic pass or destroy it with heat vision... Just one problem, he can't see through lead....



Encrypted Traffic

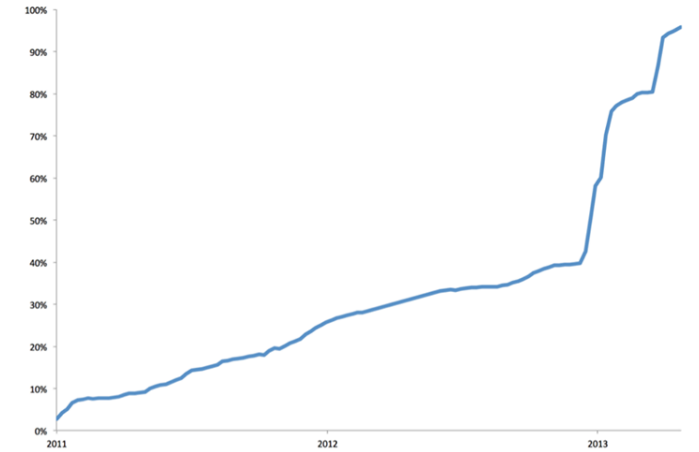


In this case, the “lead” which Superman can not see through is the Encrypted Traffic, which is the traffic making use of the HTTPS Connection.

A HTTPS Connection, is essentially a secure or private connection from the initiating application, usually a browser, all the way through the network and Internet to the destination server or site.

Encrypted Traffic

Whether it was the “Snowden Effect” & “NSA Spying Scandal”, or simply the best effort to start safeguarding our online privacy from would be attackers and thieves, a significant amount of Internet traffic today is now encrypted via the HTTPS connection. In fact there are huge initiatives to “encrypt everything”, and even Internet Search Engines, like Google, have altered their search algorithms to prioritize HTTPS sites in their search results.



Encrypt

Dell SonicWALL - Admin | <https://192.168.1.2:4430/main.html>

Apps SPARTAN GMS MEDUSA SHADOW ACHILLES DROPBOX SMA Threat Lab SmarterStats VPN

SONICWALL | Network Security Appliance Alert | Wizards | Help | Logout

Mode: Non-Config

- Dashboard
- System
- Network
- Switching
- 3G/4G
- SonicPoint
- Firewall
- Firewall Settings
- DPI-SSL
- Capture ATP
 - Status
 - Settings
- VoIP
- Anti-Spam
- VPN
- SSL VPN
- Virtual Assist
- Users
- High Availability
- Security Services
- WAN Acceleration
- AppFlow
- Log

Capture ATP / Status

Files scanned in the last 30 days

Date	Files Scanned	% of malicious files found
JA/3	5	0%
4	2	0%
5	0	0%
6	0	0%
7	0	0%
8	0	0%
9	3	0%
10	2	0%
11	4	0%
12	4	0%
13	13	0%
14	2	0%
15	2	0%
16	2	0%
17	5	0%
18	2	0%
19	2	0%
20	4	0%
21	2	0%
22	2	0%
23	2	0%
24	3	0%
25	2	0%
26	0	0%
27	4	0%
28	2	0%
29	4	0%
30	0	0%
31	22	0%
FE/1	2	0%

Viewing 13 files of 97 total scanned

Date is 01/13/2017 [Add Filter...](#)

Status	Date	Filename	Submitted by	Src	Dest
MALICIOUS	Jan 13 - 3:00pm	betabot_crypte...	C0EAE4599EA4	208.73.99.30:80	10.6.1.229:7834
MALICIOUS	Jan 13 - 3:00pm	LL_Kazy_Crypt...	C0EAE4599EA4	208.73.99.30:80	10.6.1.229:7831
MALICIOUS	Jan 13 - 2:58pm	resume.exe	C0EAE4599EA4	208.73.99.30:80	10.6.1.229:7815
MALICIOUS	Jan 13 - 11:37am	clean.exe	C0EAE4599EA4	16.30.213.121:80	10.6.1.229:7000

Status: Ready

ing purpose(s):

for details.

Issuer Statement

OK

Sizing the Opportunity



Updated - February 1, 2017
Current Firmware 6.2.5.1

SonicWALL Deployment Matrix
Confidential Information - Do No Distribute

Specification	
	TZ SOHOW
Interfaces	
1 GbE Copper	5
1 GbE SFP	0
10 GbE SFP	0
Processing Cores	2
Max Throughput (Mbps)*	50
DPI-SSL Performance	15
DPI-SSL Max Sessions	100
Max Site VPN	10
Max Remote VPN	5
Max SSL VPN	10
Max SonicPoint**	16
Max VLAN	25
SSO Users Supported	250
Max TS Servers Supported	4
Maximum DPI Connections	7500

Hardware Model	Max Concurrent DPI-SSL Connections	Hardware Model	Max Concurrent DPI-SSL Connections
SM 9600	12,000	TZ600	250
SM 9400	10,000	TZ500	250
SM 9200	8,000	TZ500W	250
NSA 6600	6,000	TZ400	250
NSA 5600	4,000	TZ400W	250
NSA 4600	3,000	TZ300	250
NSA 3600	2,000	TZ300W	250
NSA 2600	1,000	SOHO W	100

es	
9800	NSA 10800
8	0
12	10
4	6
64	96
0000	12000
0000	10000
8000	64000
5000	10000
0000	10000
50	50
N/A	N/A
512	2048
.0000	20000
N/A	N/A
2.5M	10M

IMPLEMENTING A SUCCESSFUL DEPLOYMENT

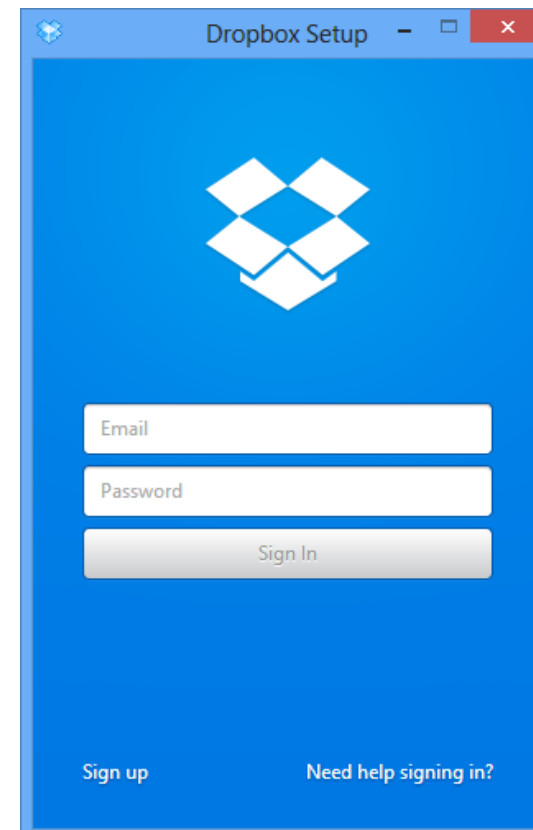
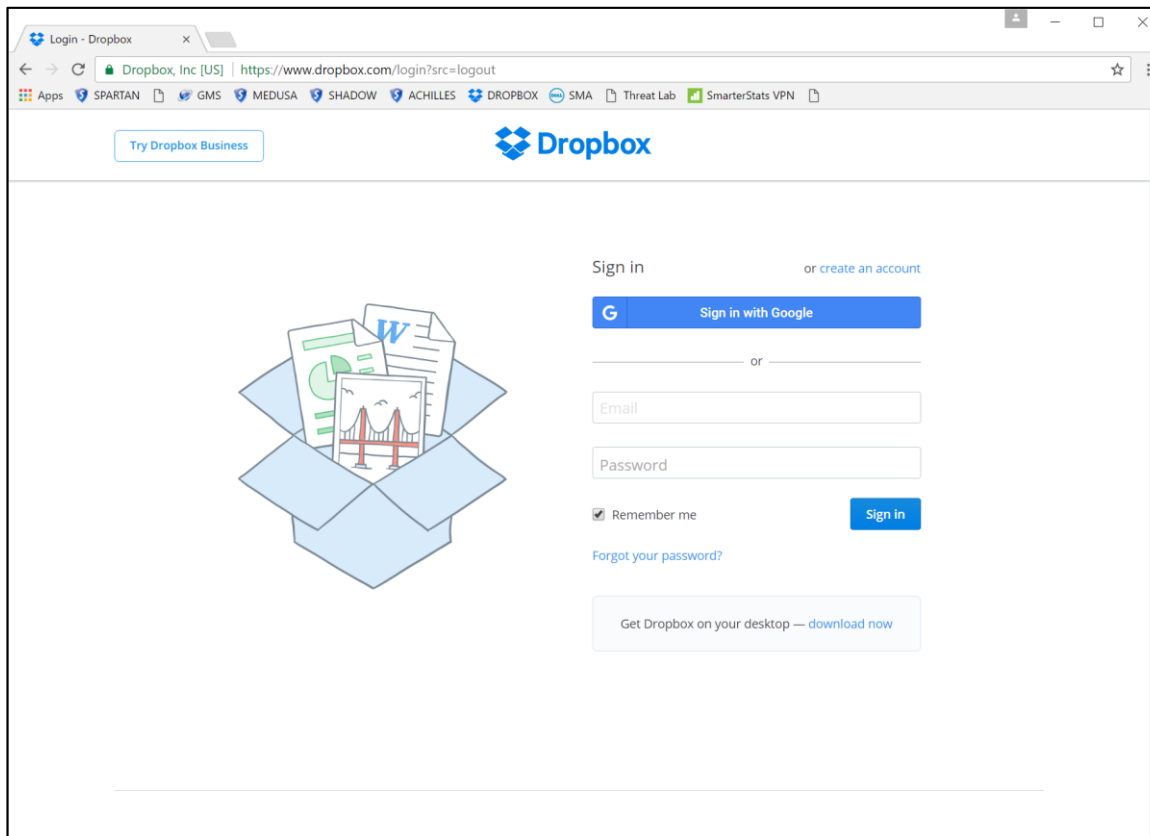
- Don't sugar coat the challenge.
- Managing the certificate deployment is the greatest challenge
- Certificate Pinning
- Automatic “excluding” broken sites & applications is a risk!
- Link to know -> <https://support.sonicwall.com/kb/sw13506>

CERTIFICATE DEPLOYMENT

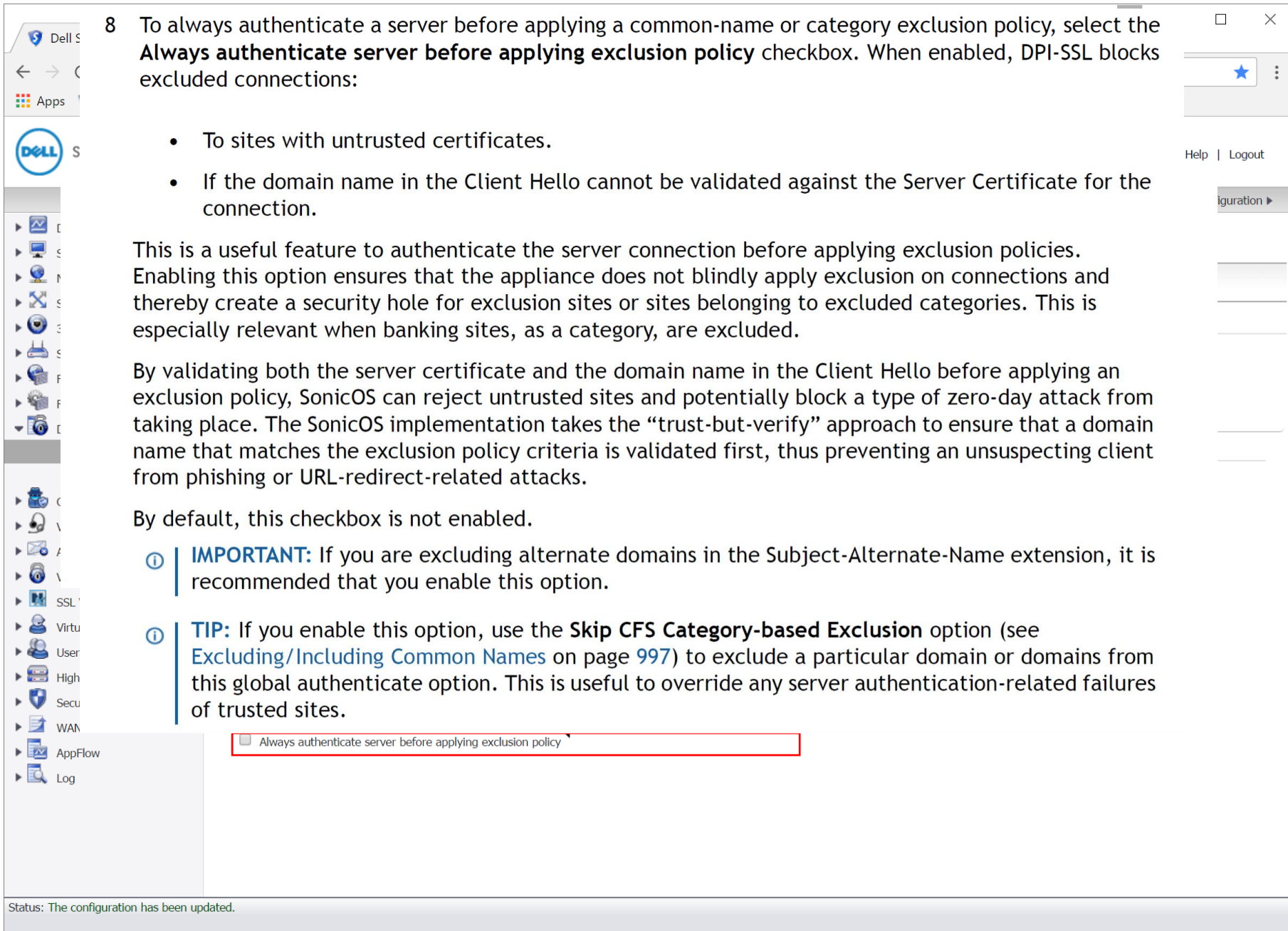
- Establishing Trust
- Operating System Certificate Store
 - Know your systems (IOS, Windows, Android, Linux)
 - Know your browsers (Firefox, Safari, Explorer, Edge, & Chrome)
- Deploying the Certificate
 - Active Directory / Group Policy
 - Trusted Devices vs. BYOD
 - Third Party Solutions / Network Access Control Solutions
 - Successful Deployments
 - Impulse
 - AirWatch
 - Clearpass

CERTIFICATE PINNING

HTTP Public Key Pinning (or certificate pinning) is a security mechanism which allows HTTPS websites to resist impersonation by attackers using mis-issued or otherwise fraudulent certificates.



THE CONFIGURATION



The screenshot shows the SonicWall configuration interface. On the left is a navigation sidebar with icons for various settings like Dell, Apps, SSL, and User. The main content area displays a configuration page with a checkbox labeled "Always authenticate server before applying exclusion policy" which is currently unchecked. A red box highlights this checkbox. At the bottom of the interface, a status message reads "Status: The configuration has been updated." On the right side of the interface, there are navigation elements including "Help | Logout" and a "Configuration" menu.

8 To always authenticate a server before applying a common-name or category exclusion policy, select the **Always authenticate server before applying exclusion policy** checkbox. When enabled, DPI-SSL blocks excluded connections:

- To sites with untrusted certificates.
- If the domain name in the Client Hello cannot be validated against the Server Certificate for the connection.

This is a useful feature to authenticate the server connection before applying exclusion policies. Enabling this option ensures that the appliance does not blindly apply exclusion on connections and thereby create a security hole for exclusion sites or sites belonging to excluded categories. This is especially relevant when banking sites, as a category, are excluded.

By validating both the server certificate and the domain name in the Client Hello before applying an exclusion policy, SonicOS can reject untrusted sites and potentially block a type of zero-day attack from taking place. The SonicOS implementation takes the “trust-but-verify” approach to ensure that a domain name that matches the exclusion policy criteria is validated first, thus preventing an unsuspecting client from phishing or URL-redirect-related attacks.

By default, this checkbox is not enabled.

- ❗ **IMPORTANT:** If you are excluding alternate domains in the Subject-Alternate-Name extension, it is recommended that you enable this option.
- ❗ **TIP:** If you enable this option, use the **Skip CFS Category-based Exclusion** option (see [Excluding/Including Common Names](#) on page 997) to exclude a particular domain or domains from this global authenticate option. This is useful to override any server authentication-related failures of trusted sites.

Always authenticate server before applying exclusion policy

Status: The configuration has been updated.

Dell SonicWALL - Admin

Not Secure | <https://192.168.1.2:4430/main.html>

Apps SPARTAN GMS MEDUSA SHADOW ACHILLES DROPBOX SMA Threat Lab SmarterStats VPN

SONICWALL Network Security Appliance Wizards | Help | Logout

Mode: Configuration ▶

- Dashboard
- System
- Network
- Switching
- 3G/4G
- SonicPoint
- Firewall
- Firewall Settings
- DPI-SSL**
 - Client SSL**
 - Server SSL
- Capture ATP
- VoIP
- Anti-Spam
- VPN
- SSL VPN
- Virtual Assist
- Users
- High Availability
- Security Services
- WAN Acceleration
- AppFlow
- Log

DPI-SSL / Client SSL

DPI-SSL Status


Current DPI-SSL connections (cur/peak/max): 0/102/4000

General Certificate Objects Common Name CFS Category-based Exclusion/Inclusion

Certificate re-signing Authority

This certificate will replace the original certificate signing authority only if that authority certificate is trusted by the firewall.
If the authority is not trusted, then the certificate will be made self-signed.
To avoid certificate errors, choose a certificate that is trusted by devices protected by DPI-SSL.

Certificate:
Default Dell SonicWALL DPI-SSL CA certificate
Default Dell SonicWALL DPI-SSL 2048 bit CA certificate
NetReaper



Status: Ready

Dell SonicWALL - Admini x

Not Secure https://192.168.1.2:4430/main.html

Apps SPARTAN GMS MEDUSA SHADOW ACHILLES DROPBOX SMA Threat Lab SmarterStats VPN

SonicWALL Network Security Appliance Alert | Wizards | Help | Logout

Mode: Configuration ▶

Dashboard
System
Network
Switching
3G/4G
SonicPoint
Firewall
Firewall Settings
DPI-SSL

Client SSL

Server SSL
Capture ATP
VoIP
Anti-Spam
VPN
SSL VPN
Virtual Assist
Users
High Availability
Security Services
WAN Acceleration
AppFlow
Log

DPI-SSL / **Client SSL**

DPI-SSL Status

Current DPI-SSL connections (concurrent/peak/max): 0/102/4000

General Certificate **Objects** Common Name CFS Category-based Exclusion/Inclusion

Exclusion/Inclusion

	Exclude:	Include:
Address Object/Group	DPI-SSL Bypass	All
Service Object/Group	None	All
User Object/Group	None	All

Status: Ready

*****Best Practice*****

Start small with the initial deployment to start identifying potential exclusions that will be required based on application and website access requirements

Dell SonicWALL - Admini x

Not Secure | <https://192.168.1.2:4430/main.html>

Apps SPARTAN GMS MEDUSA SHADOW ACHILLES DROPBOX SMA Threat Lab SmarterStats VPN

SonicWALL | Network Security Appliance Alert | Wizards | Help | Logout

Mode: Configuration ▶

- ▶ Dashboard
- ▶ System
- ▶ Network
- ▶ Switching
- ▶ 3G/4G
- ▶ SonicPoint
- ▶ Firewall
- ▶ Firewall Settings
- ▼ DPI-SSL
 - Client SSL
 - Server SSL
- ▶ Capture ATP
- ▶ VoIP
- ▶ Anti-Spam
- ▶ VPN
- ▶ SSL VPN
- ▶ Virtual Assist
- ▶ Users
- ▶ High Availability
- ▶ Security Services
- ▶ WAN Acceleration
- ▶ AppFlow
- ▶ Log

DPI-SSL / Client SSL

DPI-SSL Status

Current DPI-SSL connections (cur/pe)

Common Name Exclusions/Incl

View Style: All Built-in

#	Common Name	Action
<input type="checkbox"/>	1 .agni.lindenlab.com	
<input type="checkbox"/>	2 .atl.citrixonline.com	
<input type="checkbox"/>	3 .citrixonlinecdn.com	
<input type="checkbox"/>	4 .gotomeeting.com	
<input type="checkbox"/>	5 .iad.citrixonline.com	
<input type="checkbox"/>	6 .icloud.com	
<input type="checkbox"/>	7 .itunes.apple.com	
<input type="checkbox"/>	8 .itwin.com	
<input type="checkbox"/>	9 .las.citrixonline.com	
<input type="checkbox"/>	10 .live.citrixonline.com	Exclude
<input type="checkbox"/>	11 .livemeeting.com	Exclude
<input type="checkbox"/>	12 .logmein.com	Exclude
<input type="checkbox"/>	13 .mozilla.org	Exclude

Add Common Names

Please add new common name entries separated by comma or newline characters.

accounts.youtube.com
 clients1.google.com
 clients2.google.com
 clients3.google.com
 clients4.google.com
 commondatastorage.googleapis.com
 cros-omahaproxy.appspot.com
 dl.google.com
 dl-ssl.google.com
 gweb-gettingstartedguide.appspot.com
 m.google.com
 omahaproxy.appspot.com
 pack.google.com
 safebrowsing-cache.google.com
 safebrowsing.google.com
 ssl.gstatic.com
 storage.googleapis.com

Action: Exclude

Skip CFS Category-based Exclusion
 Skip authenticating the server

Always authenticate server before applying exclusion policy

Status: The configuration has been updated.

Dell SonicWALL - Admin | <https://192.168.1.2:4430/main.html>

SonicWALL | Network Security Appliance Wizards | Help | Logout

Mode: Non-Config ▶

- ▶ Dashboard
- ▶ System
- ▶ Network
- ▶ Switching
- ▶ 3G/4G
- ▶ SonicPoint
- ▶ Firewall
- ▶ Firewall Settings
- ▶ DPI-SSL
 - Client SSL
 - Server SSL
- ▶ Capture ATP
- ▶ VoIP
- ▶ Anti-Spam
- ▶ VPN
- ▶ SSL VPN
- ▶ Virtual Assist
- ▶ Users
- ▶ High Availability
- ▶ Security Services
- ▶ WAN Acceleration
- ▶ AppFlow
- ▶ Log

DPI-SSL / Client SSL

Connection Failure List

Browse through the list of connection failures. You can add an entry or entries as custom exclusion names, clear some or clear all entries.

	Client Address	Server Address	Common Name	Error Message
<input type="checkbox"/>	10.6.1.229	65.55.44.109	vortex-win.data.microsoft.com	Failed to authenticate cert num 1 in certificate chain for intercepted connection; Untrusted Issuer:/C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/CN=Microsoft Root Certificate Authority 2011
<input type="checkbox"/>	10.5.1.2	65.55.252.93	sqm.telemetry.microsoft.com	Server reset connection during handshake
<input type="checkbox"/>	10.5.1.2	65.55.252.93	*.big.telemetry.microsoft.com	Failed to authenticate cert num 1 in certificate chain for intercepted connection; Untrusted Issuer:/C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/CN=Microsoft Root Certificate Authority 2011
<input type="checkbox"/>	10.6.1.229	65.55.44.109	vortex-win.data.microsoft.com	Failed to authenticate cert num 1 in certificate chain for intercepted connection; Untrusted Issuer:/C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/CN=Microsoft Root Certificate Authority 2011
<input type="checkbox"/>	10.5.1.2	65.55.252.93	sqm.telemetry.microsoft.com	Server reset connection during handshake
<input type="checkbox"/>	10.6.1.229	65.55.44.109	vortex-win.data.microsoft.com	Failed to authenticate cert num 1 in certificate chain for intercepted connection; Untrusted Issuer:/C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/CN=Microsoft Root Certificate Authority 2011

Exclude Clear Clear All Close

Status: Ready

SONICWALL™

© Copyright SonicWALL

Dell SonicWALL - Admini x

Not Secure | https://192.168.1.2:4430/main.html

Apps SPARTAN GMS MEDUSA SHADOW ACHILLES DROPBOX SMA Threat Lab SmarterStats VPN

Dell SonicWALL | Network Security Appliance Alert | Wizards | Help | Logout

Mode: Non-Config ▶

- ▶ Dashboard
- ▶ System
- ▶ Network
- ▶ Switching
- ▶ 3G/4G
- ▶ SonicPoint
- ▶ Firewall
- ▶ Firewall Settings
- ▶ DPI-SSL
- ▶ Client SSL
- ▶ Server SSL
- ▶ Capture ATP
- ▶ VoIP
- ▶ Anti-Spam
- ▶ VPN
- ▶ SSL VPN
- ▶ Virtual Assist
- ▶ Users
- ▶ High Availability
- ▶ Security Services
- ▶ WAN Acceleration
- ▶ AppFlow
- ▶ Log

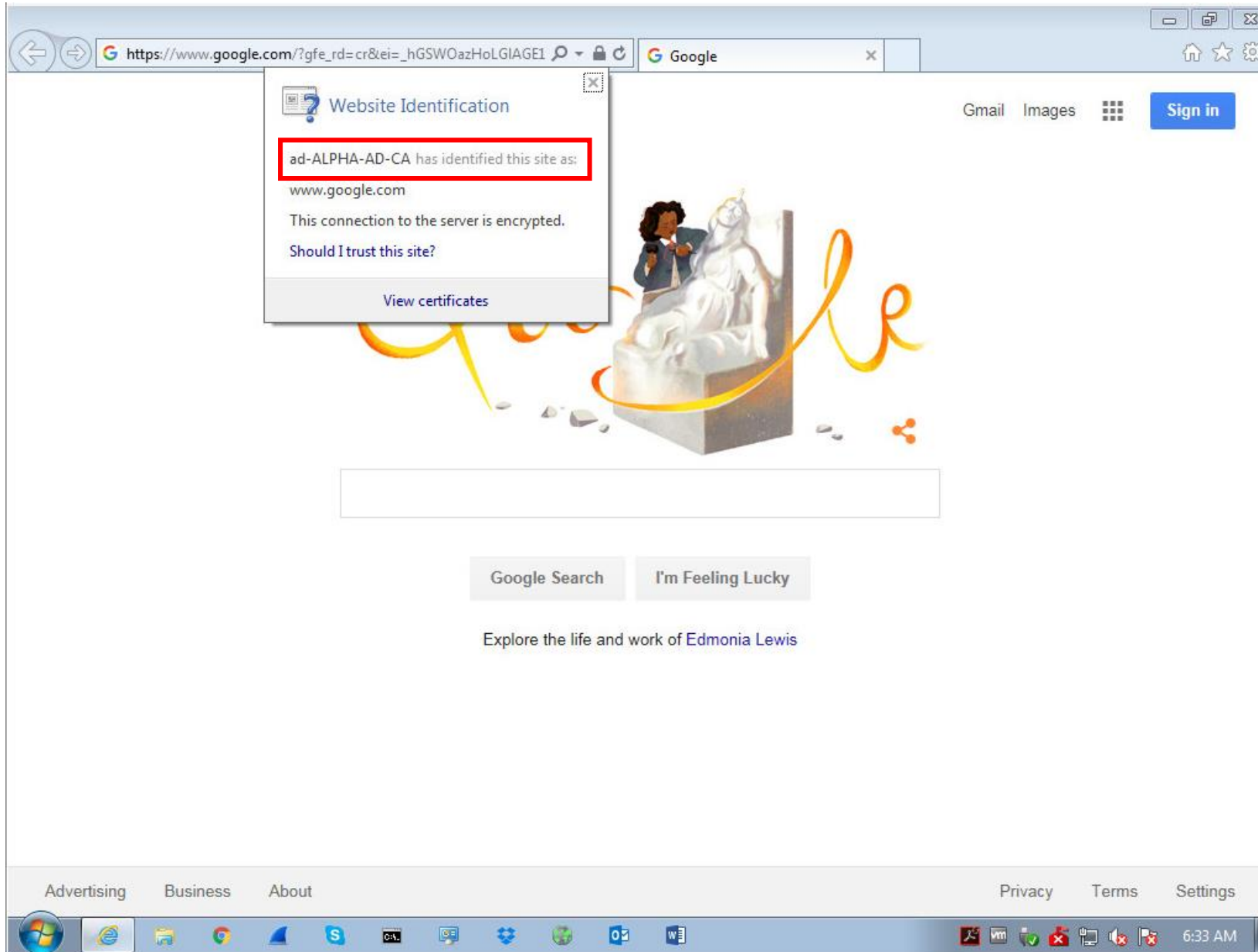
Exclude Include the following categories:

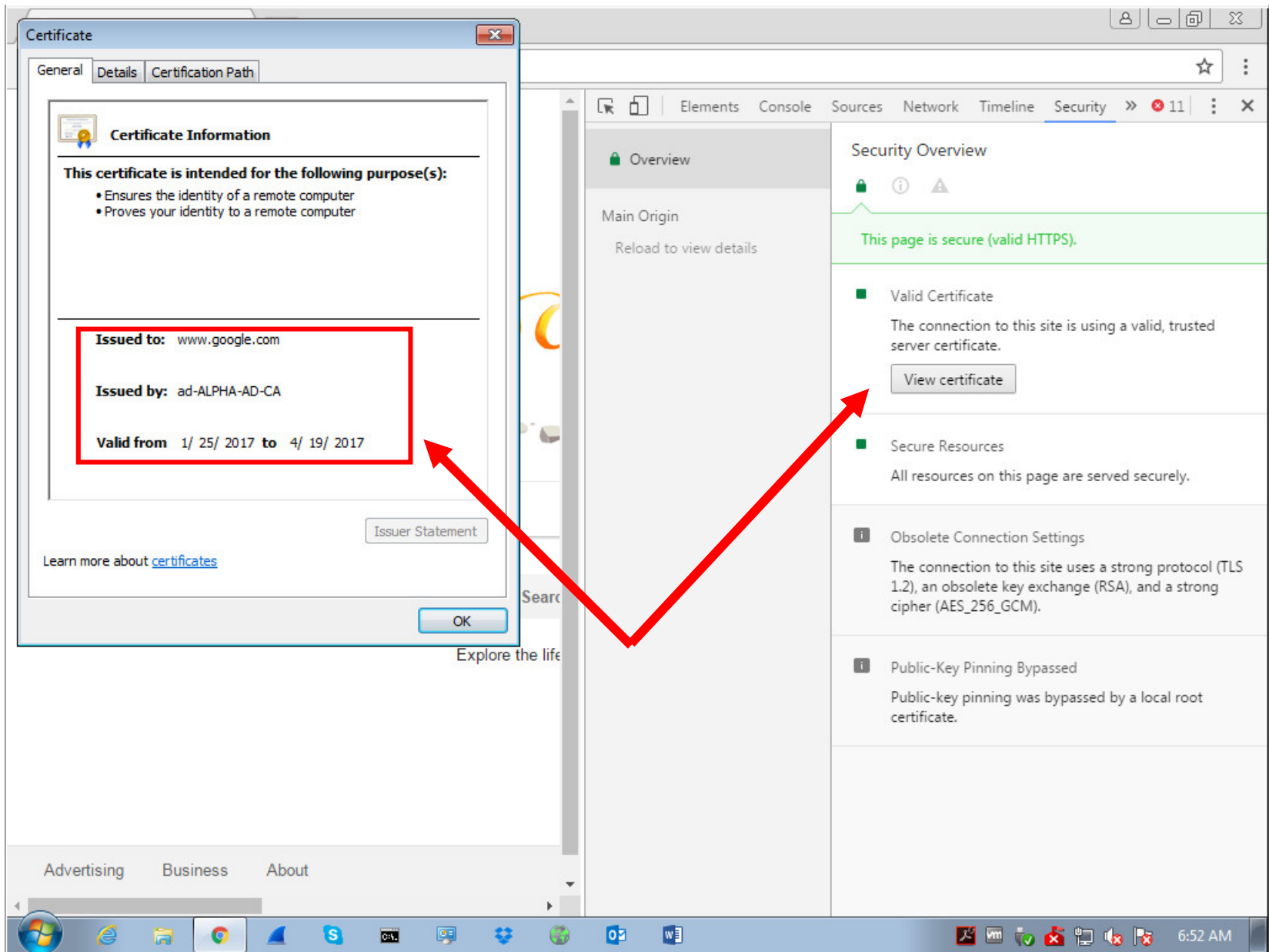
[Select all Categories](#)

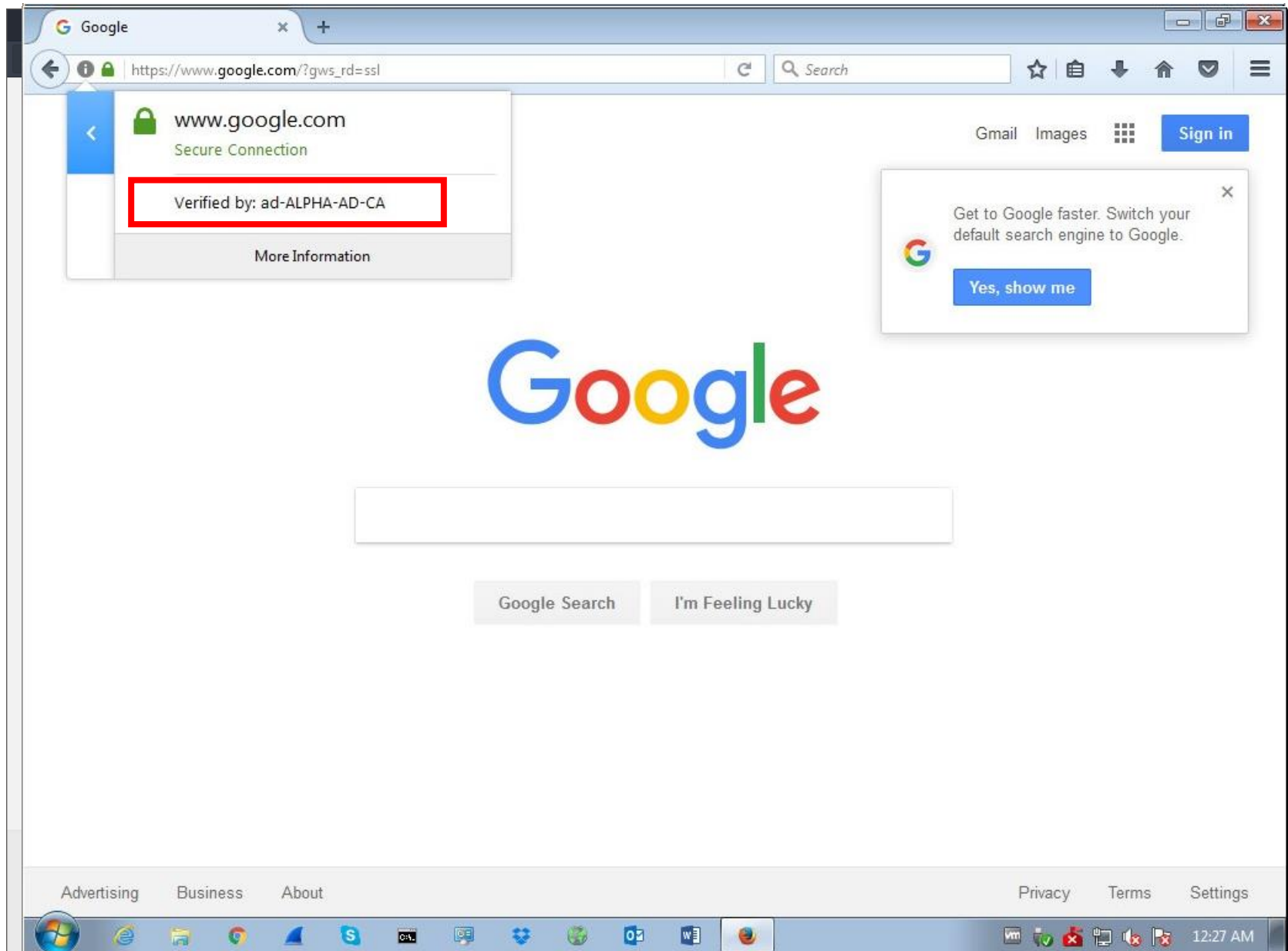
<input type="checkbox"/> 1. Violence/Hate/Racism	<input type="checkbox"/> 23. Government	<input type="checkbox"/> 45. Travel
<input type="checkbox"/> 2. Intimate Apparel/Swimsuit	<input type="checkbox"/> 24. Military	<input type="checkbox"/> 46. Vehicles
<input type="checkbox"/> 3. Nudism	<input type="checkbox"/> 25. Political/Advocacy Groups	<input type="checkbox"/> 47. Humor/Jokes
<input type="checkbox"/> 4. Pornography	<input type="checkbox"/> 26. Health	<input type="checkbox"/> 48. Multimedia
<input type="checkbox"/> 5. Weapons	<input type="checkbox"/> 27. Information Technology/Computers	<input type="checkbox"/> 49. Freeware/Software Downloads
<input type="checkbox"/> 6. Adult/Mature Content	<input type="checkbox"/> 28. Hacking/Proxy Avoidance Systems	<input type="checkbox"/> 50. Pay to Surf Sites
<input type="checkbox"/> 7. Cult/Occult	<input type="checkbox"/> 29. Search Engines and Portals	<input type="checkbox"/> 51. N/A
<input type="checkbox"/> 8. Drugs/Illegal Drugs	<input type="checkbox"/> 30. E-Mail	<input type="checkbox"/> 52. N/A
<input type="checkbox"/> 9. Illegal Skills/Questionable Skills	<input type="checkbox"/> 31. Web Communications	<input type="checkbox"/> 53. Kid Friendly
<input type="checkbox"/> 10. Sex Education	<input type="checkbox"/> 32. Job Search	<input type="checkbox"/> 54. Advertisement
<input type="checkbox"/> 11. Gambling	<input type="checkbox"/> 33. News and Media	<input type="checkbox"/> 55. Web Hosting
<input type="checkbox"/> 12. Alcohol/Tobacco	<input type="checkbox"/> 34. Personals and Dating	<input type="checkbox"/> 56. Other
<input type="checkbox"/> 13. Chat/Instant Messaging (IM)	<input type="checkbox"/> 35. Usenet News Groups	<input type="checkbox"/> 57. Internet Watch Foundation CAIC
<input type="checkbox"/> 14. Arts/Entertainment	<input type="checkbox"/> 36. Reference	<input type="checkbox"/> 58. Social Networking
<input type="checkbox"/> 15. Business and Economy	<input type="checkbox"/> 37. Religion	<input type="checkbox"/> 59. Malware
<input type="checkbox"/> 16. Abortion/Advocacy Groups	<input type="checkbox"/> 38. Shopping	<input type="checkbox"/> 60. N/A
<input type="checkbox"/> 17. Education	<input type="checkbox"/> 39. Internet Auctions	<input type="checkbox"/> 61. N/A
<input type="checkbox"/> 18. N/A	<input type="checkbox"/> 40. Real Estate	<input type="checkbox"/> 62. N/A
<input type="checkbox"/> 19. Cultural Institutions	<input type="checkbox"/> 41. Society and Lifestyle	<input type="checkbox"/> 63. N/A
<input checked="" type="checkbox"/> 20. Online Banking	<input type="checkbox"/> 42. N/A	<input type="checkbox"/> 64. Not Rated
<input checked="" type="checkbox"/> 21. Online Brokerage and Trading	<input type="checkbox"/> 43. Restaurants and Dining	
<input type="checkbox"/> 22. Games	<input type="checkbox"/> 44. Sports/Recreation	

Exclude connection if Content Filter Category is not available

Status: Ready







Questions
&
Answers

SONICWALL™

Thank you.