# Offered by NSW.net & Hitech Support

### How to access the reporting server

Navigate to <u>https://swreports.hitechsupport.com.au</u> and enter your username and password.

Note: if you are logging in for the 1<sup>st</sup> time, contact Hitech Support to setup your login and multi-factor authentication. Please call 02 8883 4355 or email support@hitechsupport.com.au

SUPPORT		
Hitech Support SonicWall GMS		
For Authorised use only		
Username:		
Password:		
Domain:	swreports •	

Enter the temporary password that was sent to you mobile phone via SMS

SUPPOR	ł	
Hitech Support Sor	icWall GMS	
For Authorised use only		
	A temporary password has been sent to your hitechsupport.com.au address. Please enter it below. Password:	

Enter your username and password again on the next screen

	SONICWALL
	Global Management System 9.1
Usernam	e
1	_
Password	1
LOGIN	
nglish   日本	語 简体中文 繁體中文 한국의 Português

#### After you have logged in, click on the Reports tab to load the reporting interface screen.

0000		Hitech WMS TZ 400 / Tin	neline				User: rico@hitech	nsupport.com.au - I	LocalDomain   E	ind Users	Logout
GlobalView Hitech WMS TZ 400	a Data Harra	Timeline		4 Sep 23, 2019 00.0	10 to Sep 23, 2019 23:59 🕴						
	Timine	•			) × (	Load Castom Repo	n. 💌				
	Initiators	Thursday								Sub	- 14
	Responders	a unevane									100
	Sarukas		1.000				100,000,000				
	Details		2,500 -		<u> </u>		- 80,000,000 72				
	Applications		.g 2,000 -				- 60,000,000 క్ర				
	User Activity		g 1,500 -				- 40,000,000	Connections			
	Web Activity		8 1,000	-			- 20,000,000	Intersterred			
	Web Filter		0	111111 V	Xaaqa	<u> </u>					
	VPN Usage		6 <sup>199</sup>	x <sup>a</sup>	7.00 18:00	70:50					
	Intrusions	Time	A Connections		Transform	-			Cost		
	▶ Botnet	1 Sep 23, 2019 00:00	1.459		304.06 KJ	3			AUD 0.00		
	▶ Geo-IP	2 Sep 23, 2019 01:00	1,468		598.09 Ki	3			AUD 0.00		
	Gateway Viruses	3 Sep 23, 2019 02:00	1,519		952.29 KI	3			AUD 0.00		
	Capture ATP	4 Sep 23, 2019 03:00	1,619		389.28 Ki				AUD 0.00		
	Spyware	5 Sep 23, 2019 04:00	1,517		330.53 KI	3			AUD 0.00		
	Attacks	6 Sep 23, 2019 05:00	1,575		410.95 Ki	3			AUD 0.00		
	h Authentication	7 Sep 23, 2019 06:00	1,624		551.48 KI	3			AUD 0.00		
	h Up (Down Status	8 Sep 23, 2019 07:00	1,584		438.03 %				AUD 0.00		
	h Custom Personte	9 Sep 23, 2019 08:00	1,611		13.99 M	3			AUD 0.01		
	- Calcon Reports	10 Sep 23, 2019 09:00	2,018		4.76 M	3			AUD 0.00		
	Analyzers	11 Sep 23, 2019 10:00	2,659		84.3 M	3			AUD 0.08		
	Configuration	12 Sep 23, 2019 11:00	2,221		43.61 M				AUD 0.04		
	Events	13 Sep 23, 2019 12:00	837		1.73 M	3			AUD 0.00		

You can select the firewall you would like to report on in the left most column – the firewall panel. Selecting an indivdual firewall will give the most detailed reports. Selecting the parent group will report on all firewalls underneath, however, it will have limited amount of reports available.

## Using the SGMS Report server

The reporting server comes with a number of simple, pre-defined reports by the software vendor. You can create your own custom reports to suit your requirements using filters and by 'drilling down' on the hyperlinks in the report.

Reports can also have the following features:

- Filters can be saved as a custom report template for reuse and scheduling;
- Moving the mouse pointer over the chart displays sample value for the intervals;
- You can sort data by clicking on the column headers.

### Filter bar

The filter bar is used to narrow the results of a report, and allows further detail to be shown. The Filter bar has pre-defined filters from a pull-down menu, which are context dependent.

+		→ ×
Add Filter		
Application Category		
Dst Interface		
Initiator Country	900,000	
Initiator Host	<u>ه</u> 200,000 -	
Initiator IP	000,000	-
Interface	Ĕ 400,000 -	
	0 200,000	

### Built in reports

### Data usage

The WMS reports shows the data usage specific to the WMS hotspot while these SGMS data usage reports displays information on everything that passes through the SonicWall firewall including the top users, host or IP addresses using the most data, and the top destinations of where data is being downloaded from.



• **<u>Timeline</u>**. Displays the data used and the amount of connections opened every hour over the period specified. The initial report is calculated on traffic going through any interface on the firewall.



- **Initiators.** Shows the top IP addresses, hosts or users that are using the most data. The initial report shows both internal and external (from the internet) initiators.
- <u>Responders.</u> Similarly, Responders shows the top destination of where data is being download from.
- <u>Services</u>. Displays the services that are being used the most from a data usage point of view.
- **Details**. This is a combination of the first four reports on one report.

### Applications

This requires a Gateway Antivirus/IPS license to be present on the firewall. This shows the applications sending or receiving traffic through the firewall.

- Data usage. Displays the amount of traffic from each application over the time period.
- **<u>Detected</u>**. Displays the applications that have been detected.
- **<u>Blocked</u>**. Displays the amount of matches to an application firewall rule where a blocking action has been specified.
- <u>Categories</u>. Displays the categories of the most common applications detected or blocked.
- <u>Initiators</u>. Shows the top IP addresses, hosts or users that are using the applications.

### **User Activity**

This displays detailed activity for user(s) that are specified in the report filter criteria. This report is only useful when some type of user authentication is being performed to the firewall, such as in a staff LAN where the SonicWall SSO agent has been deployed.

### Web Activity

These reports display detailed information about web browsing activities.

- <u>Categories.</u> Displays hits and browse time grouped by category. Note: unless a SonicWall Content Filter subscription has been purchased, the categories will be blank.
- <u>Sites</u>. Displays the top sites

	ites					2 11 =
					192.168.100.4	0 - Not Rated
					125.56.204.58	- pmw.sophos.com - Not Rated
					204.212.170.1	15 - software.sonicwall.com - Informati
		and the second se			125.56.204.35	- pmw.sophos.com - Not Rated
					125.56.204.81	- es-web-2.sophos.com - Not Rated
					125.56.205.25	- pmw.sophos.com - Not Rated
					125.56.204.21	1 - d2.sophosupd.com - Not Rated
					Cthers	
	C11 - 10					
	Site IP	Site Name	Category	Browse Time	Hits	Transferred
1	Site IP 192.168.100.40	Site Name	Category Not.Rated	Browse Time 00:04:49	Hits 193	2.38 MB
1	Site IP 192.168.100.40 125.56.204.58	Site Name	Category Not.Rated Not.Rated	Browse Time 00:04:49 00:01:07	Hits 193 45	2.38 M8 965.3 K8
1 2 3	Site IP 192.168.100.40 125.56.204.58 204.212.170.115	Site Name	Category Not Bated Not Bated Information Technol	00:04:49 00:01:07 00:01:07	Hits 193 45 8	Transferred           2.38 MB           965.3 KB           378.27 KB
1 2 3 4	SRC IP 192.168.100.40 125.56.204.58 204.212.170.115 125.56.204.35	Site Name	Category NotRated NotRated Information Techn NotRated	Browse Time 00:04:49 00:01:07 00:00:12 00:00:27	Hits 193 45 8 18	Transferred           2.38 MB           965.3 KB           378.27 KB           359.06 KB
2 2	Site IP 192.168.100.40 125.56.204.58 204.212.170.115 125.56.204.35 125.56.204.81	Site Name	Category Not.Rated Not.Rated Information Techno Not.Rated Not.Rated	Browse Time 00:04:49 00:01:07 00:00:12 00:00:27 00:01:36	Hits 193 45 8 18 64	Transferred           2.38 MB           965.3 KB           378.27 KB           359.06 KB           235.04 KB
	Site IP 192,168,100,40 125,56,204,58 204,212,170,115 125,56,204,35 125,56,204,81 125,56,205,25	ste Name omv.soshos.com software.sonicual.com omv.soshos.com cmv.soshos.com cmv.soshos.com	Category NotRated NotRated Information Techno NotRated NotRated	Browse Time 00:04:49 00:01:07 00:00:12 00:00:27 00:01:36 00:00:13	Hits 193 45 8 13 64 9	Transferred           2.38 MB           965.345           378.27 KB           339.06 KB           235.04 KB           232.96 KB
1 2 3 4 5 5 7	Site IP 192.168.100.49 125.56.204.58 204.212.170.115 125.56.204.35 125.56.204.81 125.56.205.25 125.56.205.25 125.56.204.211	Site Name  prim.sophos.com pofiniere.comcinal.com prim.sophos.com prim.sophos.com prim.sophos.com d2.sophos.com d2.sophos.com	Category NotRated NotRated Information Techn NotRated NotRated NotRated	Browse Time 00:04:49 00:01:07 20:00:12 00:00:27 00:01:36 00:00:13 00:00:46	Hits 193 45 8 18 64 9 31	Transferred           2,38 HB           965,343           376,2748           359,0648           235,0448           232,9648           235,0748

• **Initiators.** Shows the top IPs, hosts or users that are performing web browsing.

Initiators				5
				125.255.49.101 - b5165.static.pacific.net.au
				203.35.171.178 - mail.wsc.nsw.gov.au
				192.168.100.40
				192.168.1.15
				203.45.101.98
				125.255.45.88 - b4D58.static.pacific.net.au
				192.168.50.100
				Others
Initiator IP	Initiator Host	User	Connections	Transferred
1 125.255.49.10	1 b5165.static.pacific.net.	au	56	211.59 MB
2 203.35.171.17	8 mail.wsc.nsw.gov.au		81	208.56 MB
3 192.168.100.4	2		5,692	182.97 MB
4 192.168.1.15			221,183	170.62 MB
5 203.45.101.98			1	162.88 MB
6 125.255.45.88	b4D58.static.pacific.net.	au	1,008	113.08 MB

