

FortiAnalyzer Report



Report Name: 30DaySampleReport-2011-08-29-2044

Company Name: Reston TechWiz

Report Title: Firewall Monitoring Report - Reston Tech Wiz | Firewall and Network Security

Generated on: Mon Aug 29 20:44:19 2011

Scheduled Period: 2011-07-30 00:00 - 2011-08-28 23:59 EDT (FortiAnalyzer local)

Devices: WelchConstruction

Filters: None

Scheduled at: Every month 01 at 00:00



Table of Contents

Attacks on Your Network	3
Top Attacks	3
Top Attack Sources	3
Top Attack Destinations	4
Attacks by Time Period	5
Instant Messenger Information	6
Top Local IM Users	6
Internet Traffic Information	7
Top Requested Web Domains	7
Top Requested Web Pages	8
Top Allowed Web Sites	10
Top Services by Volume	11
Top Sources by Volume	12
Top Destinations by Volume	13



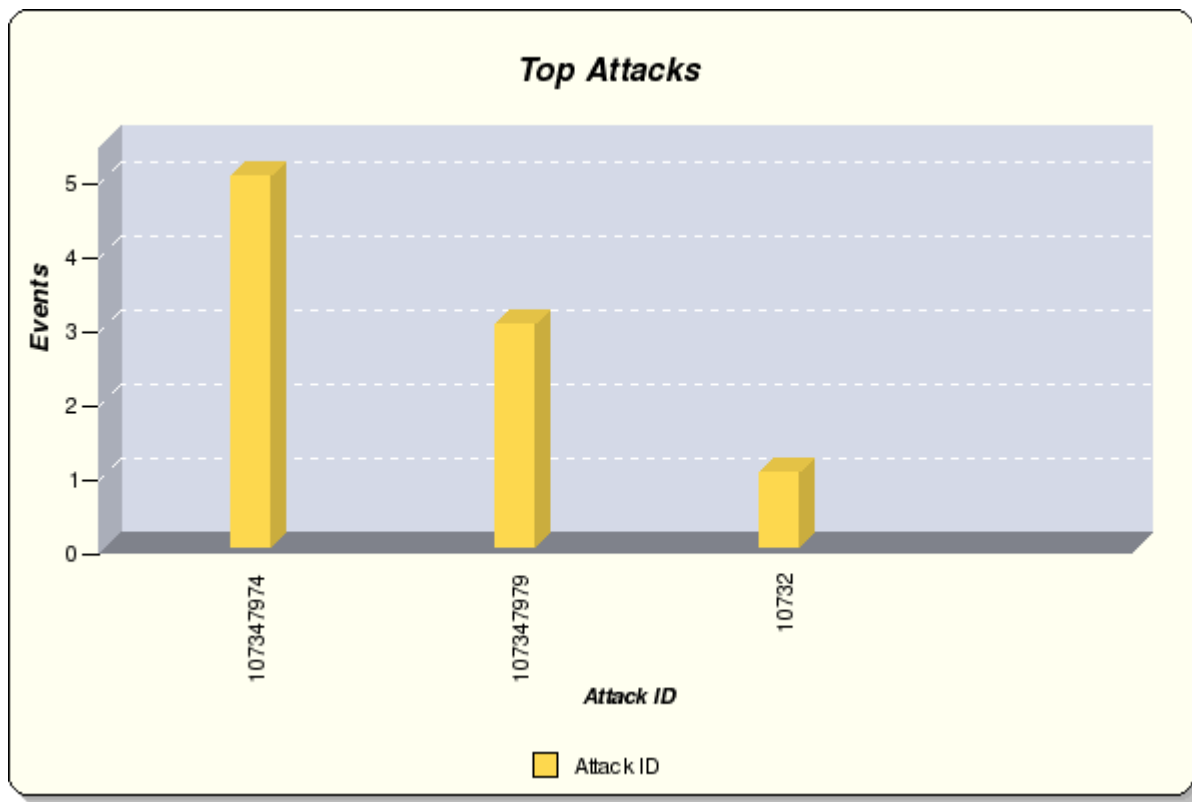
Attacks on Your Network

Top Attacks

The most frequently detected attack types over the reporting period.

WelchConstruction

Top Attacks				
Attack ID	Description	Detail	Events	% of Total
107347974	HTTP.URI.Overflow	http://www.fortinet.com/ids/ID107347974	5	55.56
107347979	HTTP.Request.Smuggling	http://www.fortinet.com/ids/ID107347979	3	33.33
10732	HTTP.Host.Header.Buffer.Overflow	http://www.fortinet.com/ids/ID10732	1	11.11
Total			9	100.00



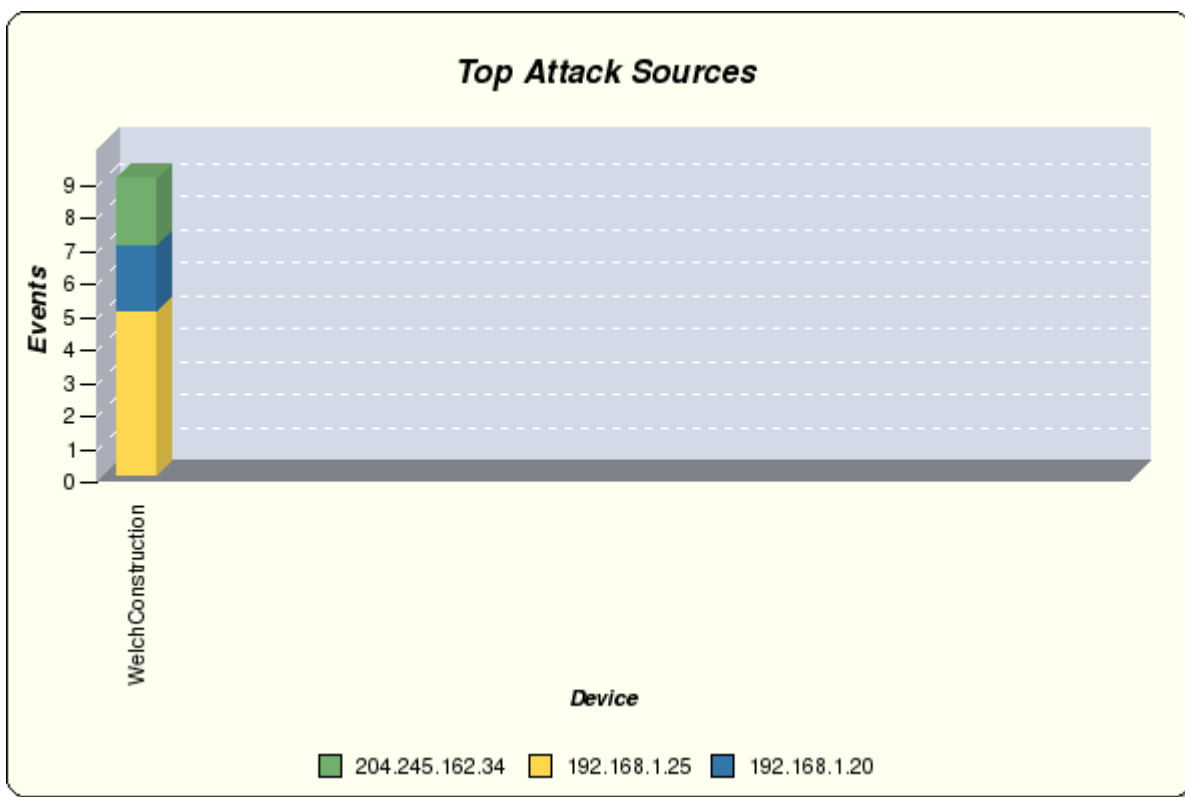
Top Attack Sources

The most frequent sources of attacks over the reporting period.



WelchConstruction

Top Attack Sources			
Device	User/Source	Events	% of Subtotal
WelchConstruction	192.168.1.25	5	55.56
	192.168.1.20	2	22.22
	204.245.162.34	2	22.22
	Subtotal	9	100.00
Total		9	100.00

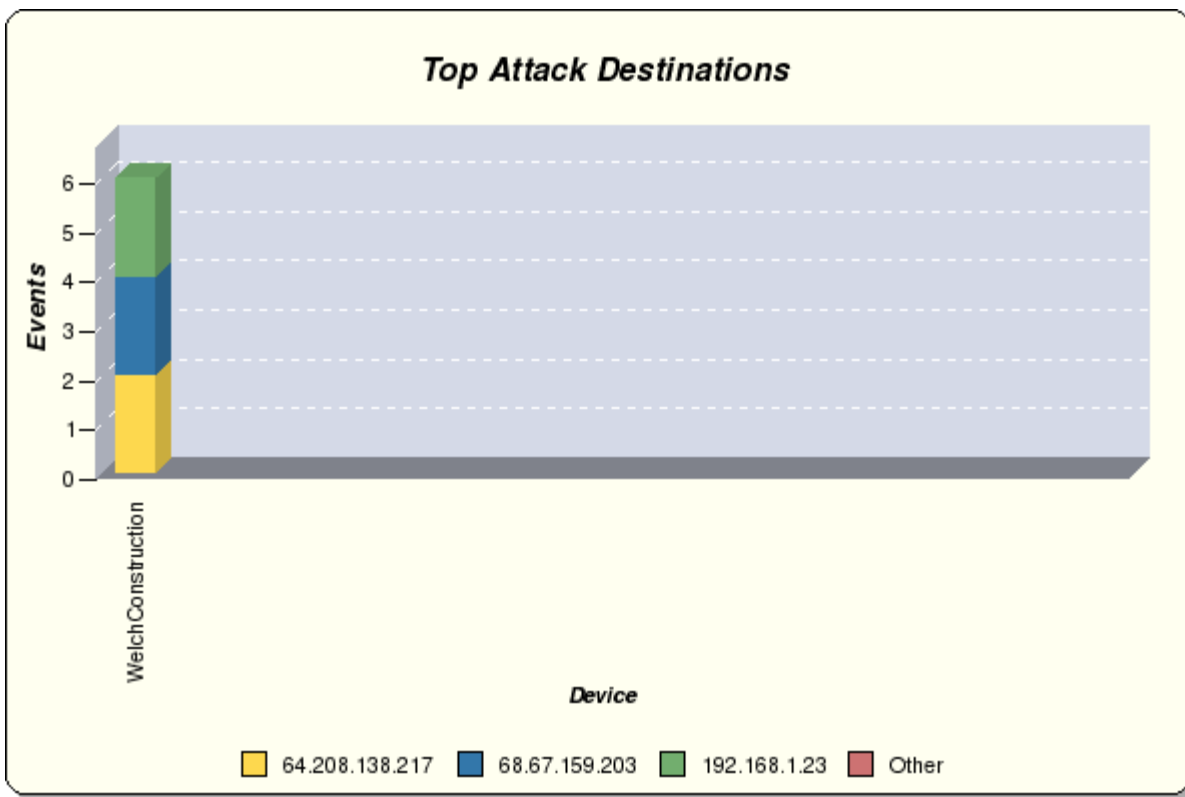


Top Attack Destinations

The most frequently attacked destinations over the reporting period.

WelchConstruction

Top Attack Destinations			
Device	Destination	Events	% of Subtotal
WelchConstruction	64.208.138.217	2	22.22
	68.67.159.203	2	22.22
	192.168.1.23	2	22.22
	Others	3	33.33
	Subtotal	9	100.00
Total		9	100.00



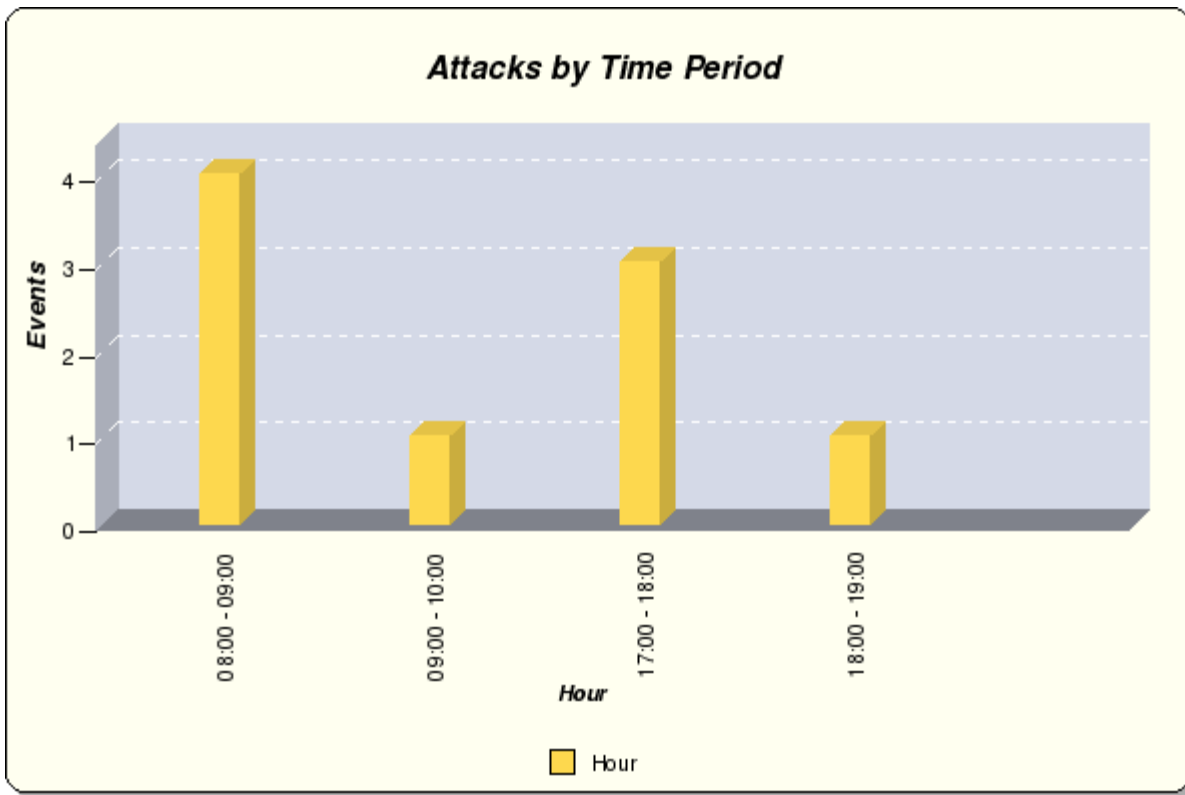
Attacks by Time Period

The time period breakdown of the number of detected attacks.

WelchConstruction

Time Scale: By Hour of Day

Attacks by Time Period		
Hour	Events	% of Total
08:00 - 09:00	4	44.44
09:00 - 10:00	1	11.11
17:00 - 18:00	3	33.33
18:00 - 19:00	1	11.11
Total	9	100.00



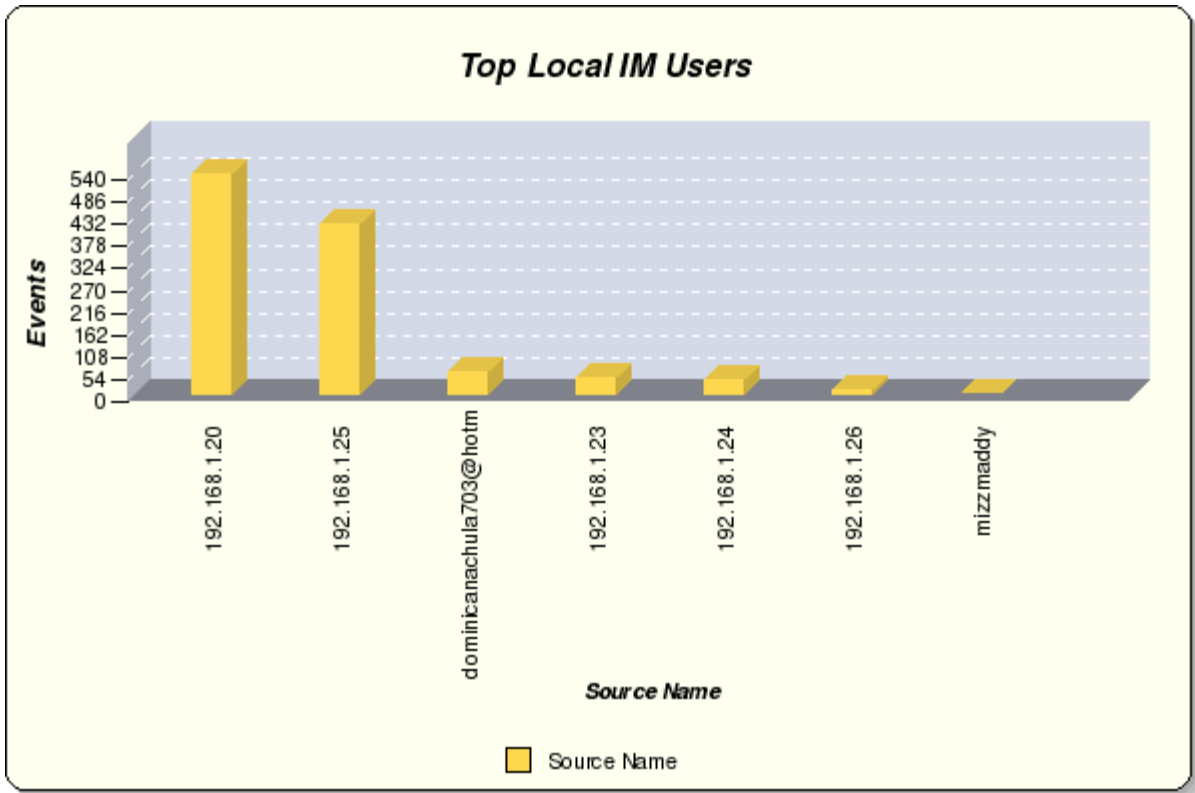
Instant Messenger Information

Top Local IM Users

The local IM users with the most connection attempts.

WelchConstruction

Top Local IM Users		
Source Name	Events	% of Total
192.168.1.20	535	49.17
192.168.1.25	413	37.96
dominicanachula703@hotmail.com	55	5.06
192.168.1.23	39	3.58
192.168.1.24	36	3.31
192.168.1.26	9	0.83
mizzmaddy	1	0.09
Total	1088	100.00



Internet Traffic Information

Top Requested Web Domains

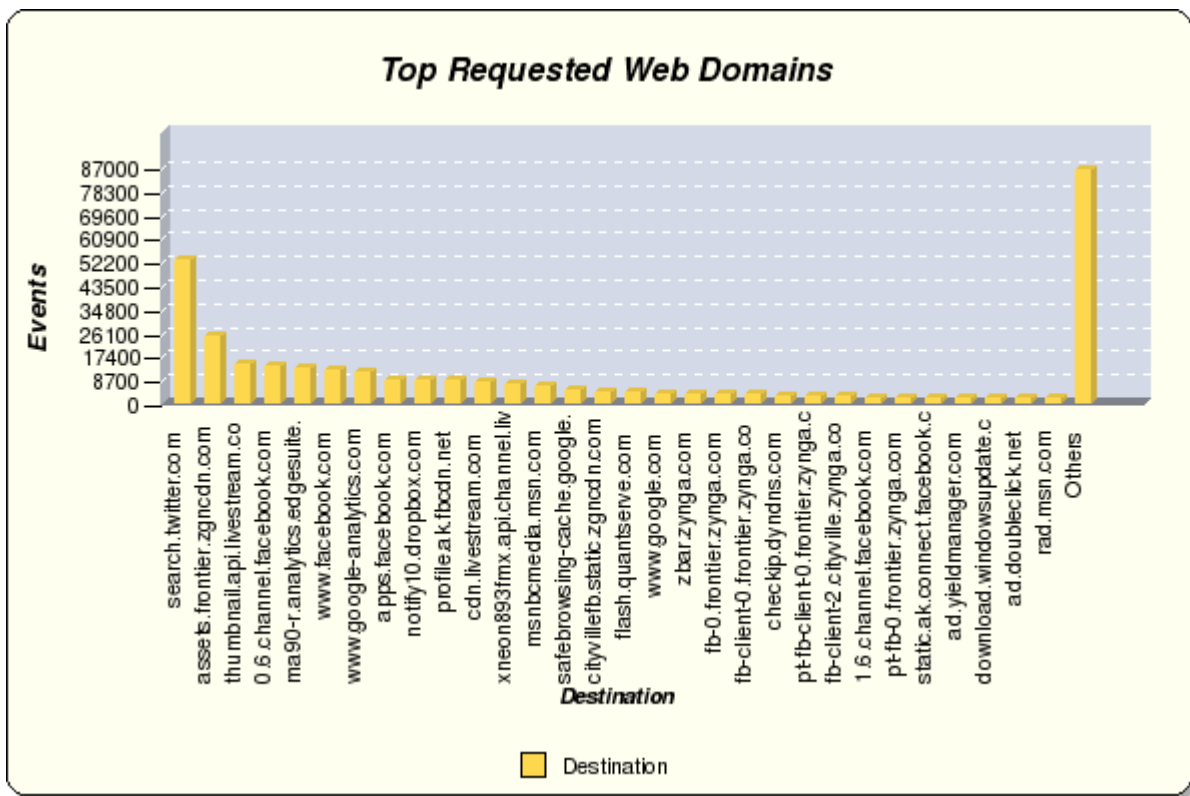
The destinations with the most web page access attempts.

WelchConstruction

Top Requested Web Domains		
Destination	Events	% of Total
search.twitter.com	52584	16.80
assets.frontier.zgncdn.com	24337	7.78
thumbnail.api.livestream.com	14011	4.48
0.6.channel.facebook.com	13227	4.23
ma90-r.analytics.edgesuite.net	12554	4.01
www.facebook.com	12006	3.84
www.google-analytics.com	10840	3.46
apps.facebook.com	8310	2.66
notify10.dropbox.com	8184	2.62
profile.ak.fbcdn.net	8014	2.56
cdn.livestream.com	7507	2.40
xneon893fmx.api.channel.livestream.com	6632	2.12



msnbcmedia.msn.com	6098	1.95
safebrowsing-cache.google.com	4633	1.48
cityvillefb.static.zgncdn.com	3928	1.26
flash.quantserve.com	3525	1.13
www.google.com	3164	1.01
zbar.zynga.com	3135	1.00
fb-0.frontier.zynga.com	2893	0.92
fb-client-0.frontier.zynga.com	2858	0.91
checkip.dyndns.com	2432	0.78
pt-fb-client-0.frontier.zynga.com	2399	0.77
fb-client-2.cityville.zynga.com	2130	0.68
1.6.channel.facebook.com	1769	0.57
pt-fb-0.frontier.zynga.com	1741	0.56
static.ak.connect.facebook.com	1664	0.53
ad.yieldmanager.com	1587	0.51
download.windowsupdate.com	1575	0.50
ad.doubleclick.net	1482	0.47
rad.msn.com	1420	0.45
Others	86270	27.57
Total	312909	100.00



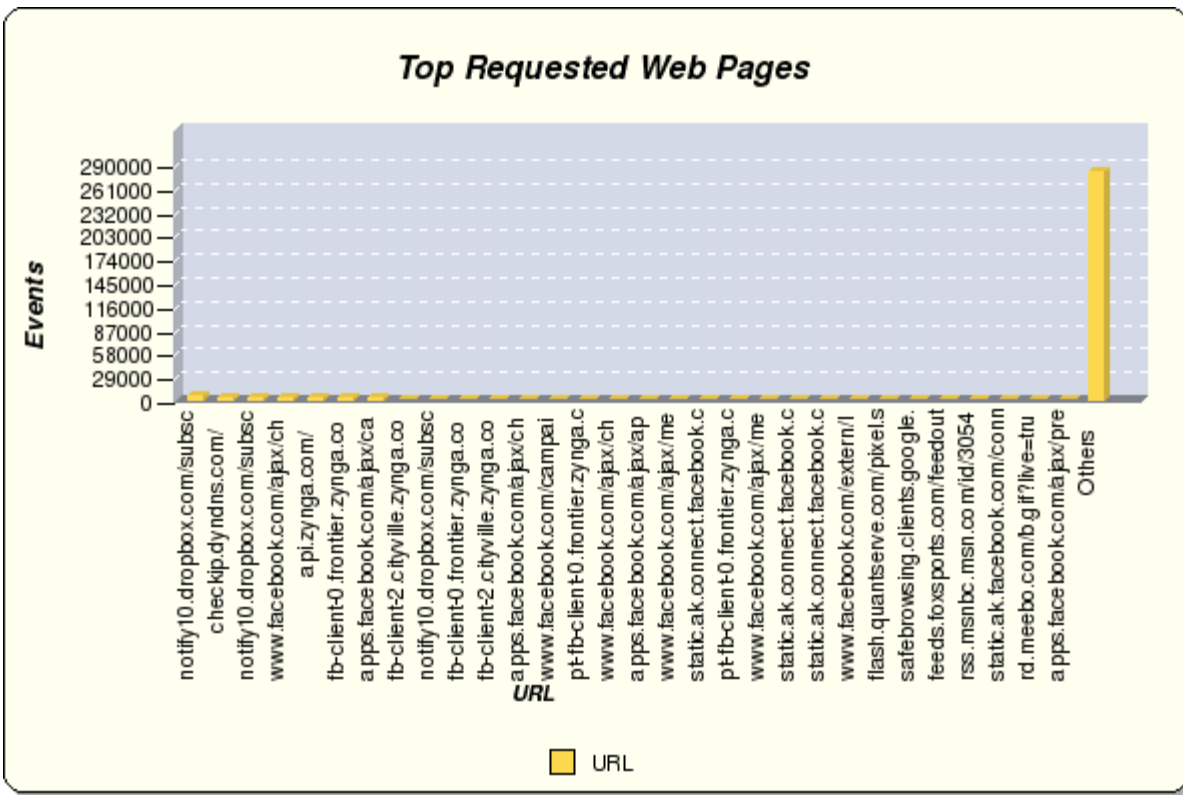
Top Requested Web Pages

The most frequently requested web pages.



WelchConstruction

Top Requested Web Pages		
URL	Events	% of Total
notify10.dropbox.com/subscribe?host_int=52151964&ns_map=57523680_390899547616,41344388_919164345732,44642822_4339610118,3883312	4929	1.58
checkip.dyndns.com/	2432	0.78
notify10.dropbox.com/subscribe?host_int=52151964&ns_map=61773969_425263536273,59173011_77368584339,41344388_919164345732,388331	2009	0.64
www.facebook.com/ajax/chat/buddy_list.php?__a=1	1764	0.56
api.zynga.com/	1334	0.43
fb-client-0.frontier.zynga.com/flashservices/gateway.php	1322	0.42
apps.facebook.com/ajax/canvas_ticker.php?__a=1	1267	0.40
fb-client-2.cityville.zynga.com/record_stats.php	1194	0.38
notify10.dropbox.com/subscribe?host_int=59133980&ns_map=57523680_390899547616,41344388_919164345732,44642822_4339610118,3883312	1151	0.37
fb-client-0.frontier.zynga.com/record_stats.php	922	0.29
fb-client-2.cityville.zynga.com/flashservices/gateway.php	898	0.29
apps.facebook.com/ajax/chat/buddy_list.php?__a=1	870	0.28
www.facebook.com/campaign/impression.php?campaign_id=177934855551844	869	0.28
pt-fb-client-0.frontier.zynga.com/flashservices/gateway.php	847	0.27
www.facebook.com/ajax/chat/send.php?__a=1	699	0.22
apps.facebook.com/ajax/apps/usage_update.php?__a=1	663	0.21
www.facebook.com/ajax/messaging/typ.php?__a=1	620	0.20
static.ak.connect.facebook.com/connect.php/en_US	597	0.19
pt-fb-client-0.frontier.zynga.com/record_stats.php	558	0.18
www.facebook.com/ajax/messaging/async.php?__a=1	542	0.17
static.ak.connect.facebook.com/connect.php/en_US/css/bookmark-button-css/connect-button-css/share-button-css/F[...]/connect-css	534	0.17
static.ak.connect.facebook.com/connect.php/en_US/js/Api/CanvasUtil/Connect/XFBML	530	0.17
www.facebook.com/extern/login_status.php?api_key=14eac7bb6f4b3019a69b01a392b72699&extern=1&channel=http%3A%2F%2Ffb-0.frontier.z	419	0.13
flash.quantserve.com/pixel.swf?pageURL=http%3A%2F%2Fwww%2Elivestream%2Ecom%2Fembed%2Fneon893fm%3FshowMoreVideos%3Dfalse%26hideI	419	0.13
safebrowsing.clients.google.com/safebrowsing/downloads?client=googlechrome&appver=13.0.782.112&pver=2.2&wrkey=AKEgNiuyd_zMygxgl	419	0.13
feeds.foxsports.com/feedout/syndicatedContent?categoryId=0&partnerKey=3Em5sEwycVHzvcQRUUiReQ	400	0.13
rss.msnbc.msn.com/id/3054049/device/rss/rss.xml	399	0.13
static.ak.facebook.com/connect.php/en_US/js/Api/CanvasUtil/Connect/XFBML	384	0.12
rd.meebo.com/b.gif?live=true&bcookie=303e723027d6c261311e&logkey=33561-989fff0a909fPHJO5Syy&meeboConnect=false&uid=true&partner	381	0.12
apps.facebook.com/ajax/presence/update.php?__a=1	351	0.11
Others	283186	90.50
Total	312909	100.00

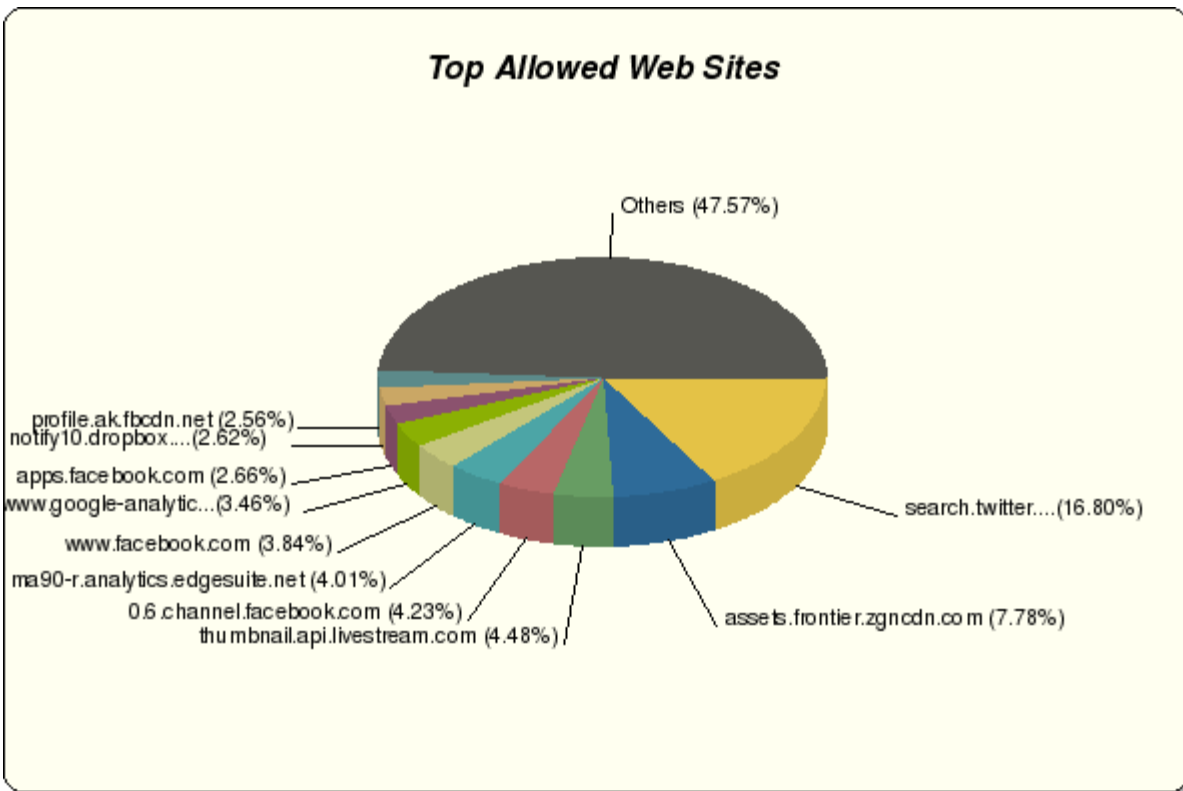


Top Allowed Web Sites

The most frequently allowed web sites over the reporting period.

WelchConstruction

Top Allowed Web Sites		
Destination	Events	% of Total
search.twitter.com	52584	16.80
assets.frontier.zgncdn.com	24337	7.78
thumbnail.api.livestream.com	14011	4.48
0.6.channel.facebook.com	13227	4.23
ma90-r.analytics.edgesuite.net	12554	4.01
www.facebook.com	12006	3.84
www.google-analytics.com	10840	3.46
apps.facebook.com	8310	2.66
notify10.dropbox.com	8184	2.62
profile.ak.fbcdn.net	8014	2.56
Others	148842	47.57
Total	312909	100.00

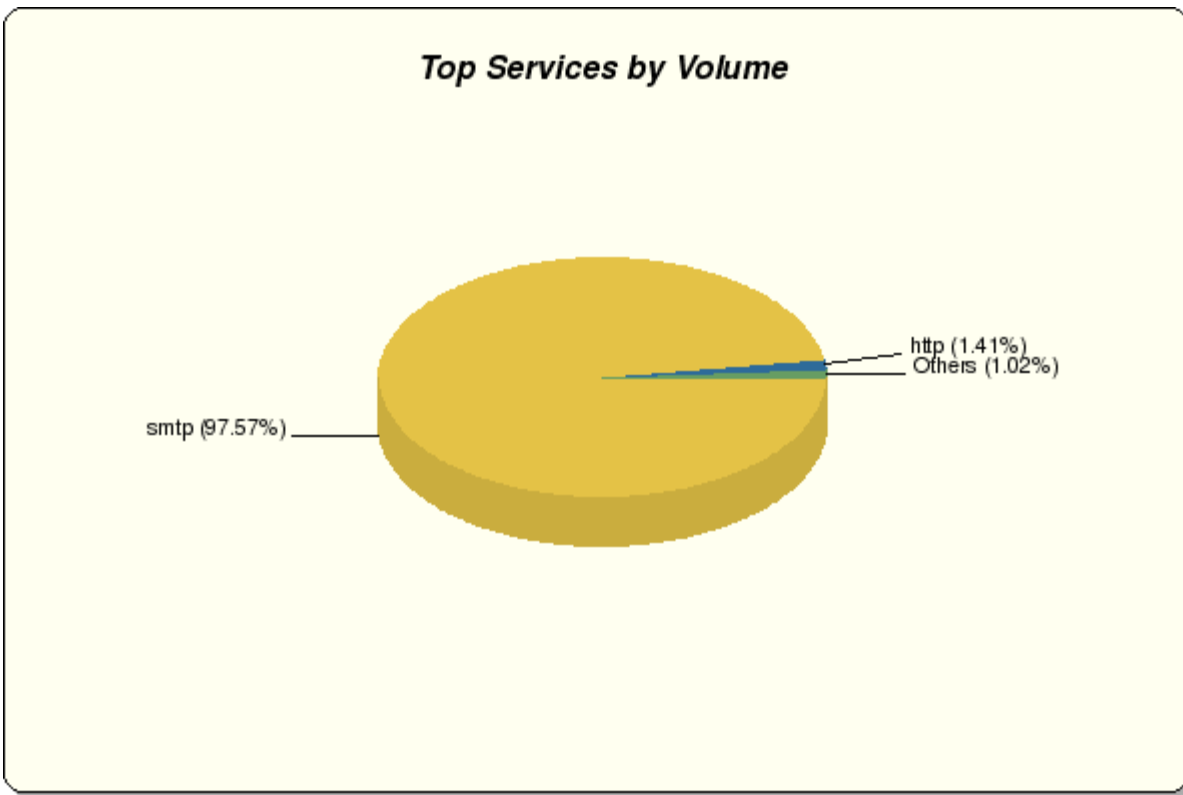


Top Services by Volume

The Internet services with the most traffic volume over the reporting period.

WelchConstruction

Top Services by Volume		
Service	Traffic (MB)	% of Total
smtp	362208.88	97.57
http	5238.57	1.41
imaps	2438.32	0.66
https	651.38	0.18
6020/tcp	256.70	0.07
microsoft-ds	215.85	0.06
ftp	84.00	0.02
1935/tcp	42.78	0.01
dns	19.39	0.01
2525/tcp	15.93	0.00
Others	60.54	0.02
Total	371232.32	100.00

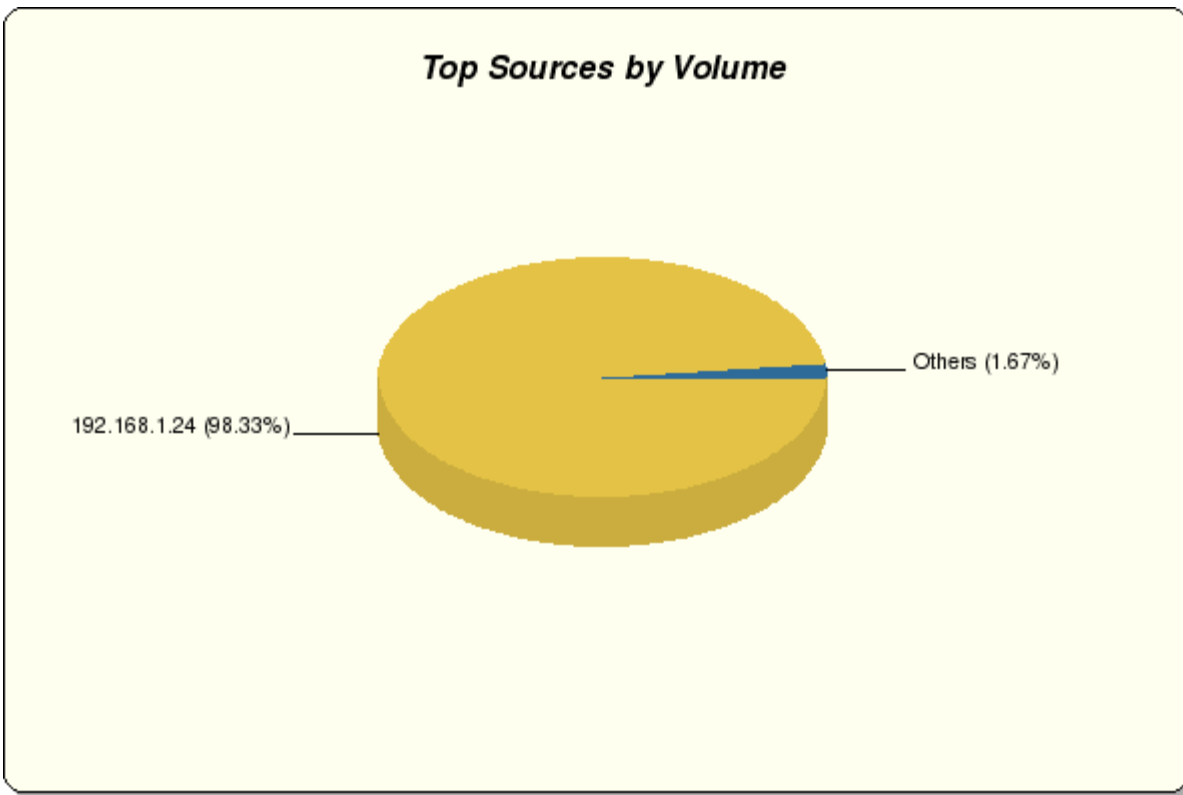


Top Sources by Volume

The sources with the most traffic volume over the reporting period.

WelchConstruction

Top Sources by Volume		
User/Source	Traffic (kB)	% of Total
192.168.1.24	373789998.24	98.33
192.168.1.20	2547960.50	0.67
192.168.1.25	1531536.13	0.40
192.168.1.23	1123011.80	0.30
192.168.1.26	799299.78	0.21
192.168.1.3	220681.20	0.06
192.168.1.31	92520.93	0.02
192.168.1.29	19364.87	0.01
192.168.1.28	16325.19	0.00
192.168.1.2	1101.02	0.00
Others	99.93	0.00
Total	380141899.60	100.00



Top Destinations by Volume

The destinations with the most traffic volume over the reporting period.

WelchConstruction

Top Destinations by Volume		
Destination	Traffic (MB)	% of Total
gw-in-f108.1e100.net	357326.21	96.25
gx-in-f108.1e100.net	6905.57	1.86
a204-245-162-48.deploy.akamaitechnologies.com	546.28	0.15
212-105.livestream.com	455.53	0.12
gy-in-f109.1e100.net	380.05	0.10
212-106.livestream.com	270.24	0.07
173.193.216.92-static.reverse.softlayer.com	257.64	0.07
a204-245-162-58.deploy.akamaitechnologies.com	252.70	0.07
a204-245-162-40.deploy.akamaitechnologies.com	229.95	0.06
192.168.1.150	216.47	0.06
Others	4391.68	1.18
Total	371232.32	100.00



Top Destinations by Volume

