

## Application Control

Fortinet provides robust application control reports detailing how applications are traversing your network and the risks they might pose. These are useful when trying to determine how to define/optimize firewall policies, utilize corporate resources or conduct internal trainings. For instance, the excessive use of Dropbox might indicate the need to setup an internal file repository. Similarly, an uptick in social networking activity may indicate the need for trainings or reminders of corporate policies.

## Applications Detected by Risk Behavior

Modern security organizations need increasingly complex security processes in place to handle the myriad of applications in use on the network and in the data center. The problem is determining which applications in your environment are most likely to cause harm. The following charts provide a breakdown of the high risk applications identified on the network. It has been determined by FortiGuard Labs that these applications represent possible vectors for data compromise, network intrusion, or a reduction in network performance.

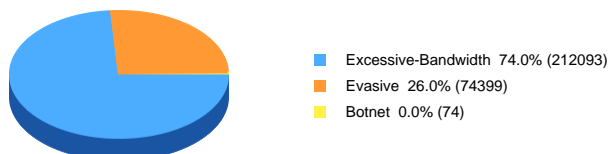
Risk	Application Name	Category	Technology	Bandwidth	Sessions
Botnet	Zeroaccess.Botnet	Botnet	Client-Server	24.07 KB	74
Evasive	Skype	P2P	Peer-to-Peer	7.42 MB	22.11 K
Evasive	WebEx	Collaboration	Browser-Based Client-Server	51.86 MB	21.80 K
Evasive	Dropbox	File.Sharing	Browser-Based	10.30 GB	13.34 K
Evasive	Google.Docs	Collaboration	Browser-Based	1.43 MB	4.29 K
Evasive	Google.Desktop	General.Interest	Client-Server	1.69 GB	2.18 K
Evasive	Skype_Communication	P2P	Peer-to-Peer	725.86 KB	2.18 K
Evasive	EBay.Toolbar	General.Interest	Browser-Based	365.95 KB	1.10 K
Evasive	Evernote	General.Interest	Browser-Based	222.32 KB	657
Evasive	RDP	Remote.Access	Client-Server	502.28 MB	636

## Application Usage By Category

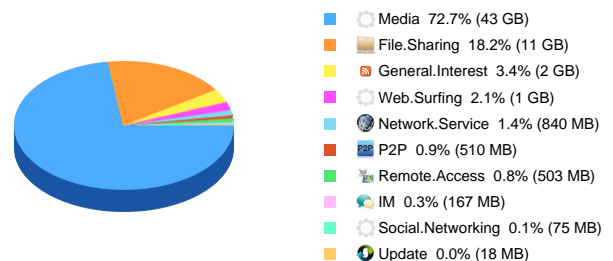
As part of the traffic classification process, the FortiGate identifies and categorizes applications crossing the network into different categories based on the number of sessions and bandwidth used. This data complements the granular application threat data and provides a more complete summary of the types of applications in use on the network.

Application Category	Bandwidth
Media	43.11 GB
File.Sharing	10.79 GB
General.Interest	2.01 GB
Web.Surfing	1.25 GB
Network.Service	840.21 MB
P2P	510.11 MB
Remote.Access	502.66 MB
IM	167.36 MB
Social.Networking	74.92 MB
Update	18.25 MB

## Risky Applications Breakdown



## Application Usage By Category



## Malware and Other Threats

FortiGate users have visibility into the types of malicious activity being blocked on their networks and can cross reference with the award-winning FortiGuard botnet, virus and IPS research center. Determining which inbound attacks are being prevented and which users are frequent targets can be invaluable in mobilizing your network defenses. For instance, if a specific user is the consistently a malware victim, you can either provide individual guidance or block that user from specific activities.

### Top Malware Crossing The Network

FortiGate monitors the network for viruses that are in transit. The FortiGate is able to apply different strategies in order to detect malware: signatures using Fortinet's Compact Pattern Recognition Language (aka CPRL) and heuristics which are applied to file structures and API calls. The FortiGate's antivirus engine provides two main capabilities: decompression which allows embedded files to be extracted and emulation which allows the hidden layers of malicious files to be extracted.

Virus Name	Occurrences
W32/FakeAV.OY!tr	15746
W32/Simda.B!tr	15613
W32/Zbot.ANMI!tr	15523
W32/Jorik.EF78!tr	15521
W32/Agent.RNI!tr	15439
JS/Redirector.M!exploit	15256
W32/Zbot.DHN!tr	15224

### Top Virus Victims

This visualization provides information about which network users are more prone to infection from viruses. It enables direct identification of the host(s) that are creating sources of malicious traffic on the network. The following chart displays the counter of the number of viruses per end user.

Virus Victims	Occurrences
shiggins	878
paltidore	875
ryoung	875
lbarker	875
lcorrales	875
hrosenberg	874
glucas	873
iaustin	873
iholden	873
smetcalf	872
wjones	870
jgupta	868
hdonoso	867
ringram	866
hstiglitz	865

## Web Usage and Browsing Habits

The manner in which corporate users interact with specific websites and with certain web categories can be very revealing. FortiGates are able to determine which websites are being frequented, how long those sites are being browsed and the classifications of websites being accessed. Administrators are able to optimize their firewall policies to ensure that employees can get to the information they need while complying with corporate use policies.

### Top Websites Visited By Network Users

Identifying and managing the top URLs visited by network users provides greater visibility and control, and subsequently, better network security. By leveraging Fortinet threat prevention, application control and URL filter technologies, the volume of web sites by category can be reviewed and strategies can be put in place to prevent users accessing sites considered to be a risk to overall network security.

Domain	Category	Visits
youtube.com	Streaming Media and Download	86111
wikipedia.org	Reference	43777
craigslist.org	Shopping and Auction	32751
facebook.com	Social Networking	25366
skype.com	Instant Messaging	24282
google.com	Web-based Email	22176
pandora.com	Internet Radio and TV	21952
webex.com	Information Technology	21803
linkedin.com	Business	19730
amazon.com	Shopping and Auction	16004

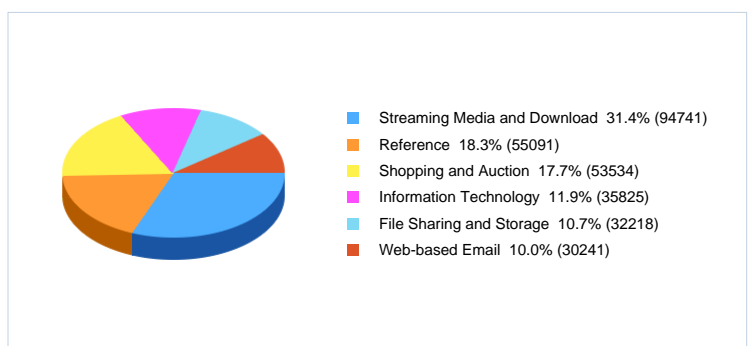
### Top Websites By Browsing Time

The following chart shows the web sites that users visit for extended periods of time. The administrator can then decide to create security policies to mitigate or block website access, accordingly to their internal corporate use policies.

Website	Browse Time (min)	Bandwidth	Traffic Sent	Traffic Received
en.wikipedia.org	95.41			14.66 MB
craigslist.org	87.65			10.99 MB
youtube.com	85.58			30.82 GB
youtube.com	85.46			94.03 MB
mail.google.com	66.47			7.42 MB
skype.com	66.46			7.42 MB
stream.pandora.com	66.27			52.28 MB
webex.com	65.12			51.86 MB
facebook.com	60.05			47.50 MB
linkedin.com	59.40			6.61 MB

### Top Web Categories

User browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate an inefficient optimization of web filtering policies. It can also give some insight into the general web browsing habits of corporate users and assist in defining corporate compliance guidelines. This chart details web categories by the number of times URLs within those categories were requested and by the number of bandwidth used.


















## Bandwidth and Network Usage

While the use of technologies such as video streaming and peer to peer have positively impacted businesses, many administrators must ensure that a proper balance is being met. Some employees may significantly utilize more bandwidth than others thus affecting monthly bandwidth costs and reducing the network efficiency of others. This can easily be alleviated by keeping an eye on individual bandwidth usage and enacting traffic shaping or blocking certain applications when necessary.
















### Top Application Users By Bandwidth

This chart provides information about the users who are creating the most network traffic in terms of bandwidth usage. It helps the network administrator to identify users that are potentially abusing network usage or creating traffic that does not comply with internal security policies.

User (or IP)	Source IP	Bandwidth	Traffic Out	Traffic In
 kmcallister	192.168.10.167	<div><div></div></div>		219.86 MB
 cosullivan	192.168.10.59	<div><div></div></div>		203.91 MB
 kfuller	192.168.10.215	<div><div></div></div>		196.18 MB
 lsilva	192.168.10.129	<div><div></div></div>		194.77 MB
 pwashburn	192.168.10.205	<div><div></div></div>		192.03 MB
 woneill	192.168.10.203	<div><div></div></div>		190.98 MB
 gmcclung	192.168.10.65	<div><div></div></div>		190.44 MB
 lbarker	192.168.10.2	<div><div></div></div>		189.83 MB
 hdonoso	192.168.10.28	<div><div></div></div>		187.23 MB
 pwashburn	192.168.10.139	<div><div></div></div>		185.99 MB
 bgore	192.168.10.214	<div><div></div></div>		185.32 MB
 awinters	192.168.10.235	<div><div></div></div>		185.29 MB
 rporter	192.168.10.64	<div><div></div></div>		184.87 MB
 kali	192.168.10.52	<div><div></div></div>		184.57 MB
 ckinnison	192.168.10.107	<div><div></div></div>		184.49 MB

### Top Application Users By Sessions

The section below illustrates the quantity of network users who are opening the highest number of connections. This is a critical value because some users could be opening multiple sessions without their knowledge (e.g. botnets). Statistics on the amount of sessions a user has opened and the bandwidth of those sessions is recorded by the FortiGate.

User (or IP)	Source IP	Sessions
 kmcallister	192.168.10.167	1954
 woneill	192.168.10.203	1935
 tbrown	192.168.10.58	1703
 dsimpson	192.168.10.162	1697
 bmatsubara	192.168.10.26	1691
 cloomis	192.168.10.156	1690
 emccrary	192.168.10.240	1687
 cloomis	192.168.10.11	1683
 pharris	192.168.10.244	1683
 cullman	192.168.10.89	1682
 lbarker	192.168.10.2	1682
 jkirovski	192.168.10.247	1676
 hdonoso	192.168.10.28	1674
 chall	192.168.10.205	1671
 iholden	192.168.10.202	1669