



Cyber Threat Assessment Report

Vital Statistics

This document provides the findings of a recent analysis of your infrastructure. The document represents a summary of these findings and presents a set of recommendations for addressing the detected events. The analysis is based on data collected using the characteristics below:

Company Details

Company Name: Black Hat Conference

Location: Las Vegas, NV, US

Industry: Network Security

Company Size: 9,000+ attendees

Test Details

Test Start Date: July 30, 2016

Test Duration: 6 Day(s)

FortiGate Model: FG 1500D

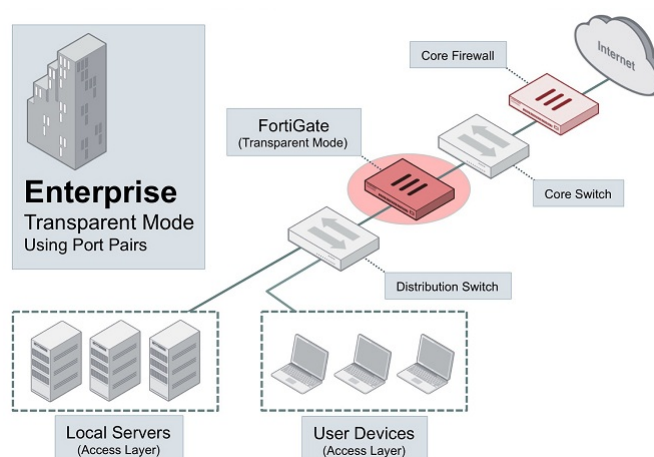
FortiOS Firmware: FortiOS 5.4.0

Network Analyzed: Network Operations Center

Functions Enabled: Antivirus, App Control, IPS, Traffic, Web

Deployment and Methodology

Your network was monitored with a FortiGate 1500D in Transparent Mode (Port Pair) mode. This is a non-invasive way to intercept traffic as it moves over your network.



During your assessment, network activity was monitored as it passed through your infrastructure. While traffic logs record much of the session information flowing across your network, FortiGates can also monitor more in-depth security logging such as IPS, anti-virus, web and application control. This assessment was created based on telemetry from all log types and provides an overview of your network's activity. Used in conjunction with FortiAnalyzer, FortiGates can provide additional functions such as event management (e.g. alerts), FortiView analytics (e.g. investigating specific user activity) and reporting.

Executive Summary



IPS Attacks Detected: 38,800

Malware/Botnets Detected: 108

High-Risk Applications Used: 80

Malicious Websites Detected: 1,087

Last year, over 2,100 enterprises were breached as a result of poor internal security practices and latent vendor content security. The average cost of a corporate security breach is estimated at \$3.5 million USD and is rising at 15% year over year. Intrusions, malware/botnets and malicious applications collectively comprise a massive risk to your enterprise network. These attack mechanisms can give attackers access to your most sensitive files and database information. FortiGuard Labs mitigates these risks by providing award-winning content security and is consistently rated among industry leaders by objective third parties such as NSS Labs, VB 100 and AV Comparatives.



Applications Detected: 779

Top Used Application: Google.Groups

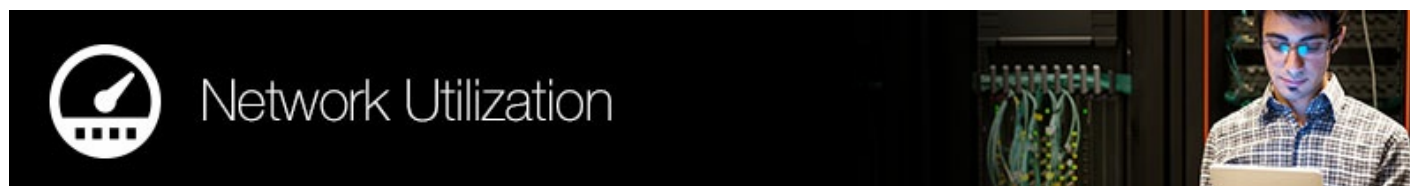
Top Application Category: Network.Service

Websites Visited: 463,204

Top Website: vid-io.springserve.com

Top Web Category: Information Technology

User application usage and browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate a lack of proper enforcement of corporate usage policies. Most enterprises recognize that personal use of corporate resources is acceptable. But there are many grey areas that businesses must keep a close eye on including: use of proxy avoidance/peer to peer applications, inappropriate web browsing, phishing websites, and potentially illegal activity - all of which expose your company to undue liability and potential damages. With over 5,800 application control rules and 250 million categorized websites, FortiGuard Labs provides telemetry that FortiOS uses to keep your business running effectively.



Total Bandwidth: 11.09 TB

Top Host by Bandwidth: 10.168.1.4

Performance effectiveness is an often undervalued aspect of security devices, but firewalls must keep up with the line speeds that today's next generation switches operate at. A recent survey by Infonetics indicates that 77% of decision-makers at large organizations feel that they must upgrade their network security performance (100+ Gbps aggregate throughput) in the coming year. FortiGates leverage FortiASICs to accelerate CPU intensive functions such as packet forwarding and pattern matching. This offloading typically results in a 5-10X performance increase when measured against competitive solutions.

Recommended Actions

Application Vulnerability Attacks Detected (372)

Application vulnerabilities (also known as IPS attacks) act as entry points used to bypass security infrastructure and allow attackers a foothold into your organization. These vulnerabilities are often exploited due to an overlooked update or lack of patch management process. Identification of any unpatched hosts is the key to protecting against application vulnerability attacks.

Malware Detected (105)

Malware can take many forms: viruses, trojans, spyware/adware, etc. Any instances of malware detected moving laterally across the network could also indicate a threat vector originating from inside the organization, albeit unwittingly. Through a combination of signature and behavioral analysis, malware can usually be prevented from executing and exposing your network to malicious activity. Augmenting your network with APT/sandboxing technology (e.g. FortiSandbox) can also prevent previously unknown malware (zero-day threats) from propagating within your network.

Botnet Infections (3)

Bots can be used for launching denial-of-service (DoS) attacks, distributing spam, spyware and adware, propagating malicious code, and harvesting confidential information which can lead to serious financial and legal consequences. Botnet infections need to be taken seriously and immediate action is required. Identify botnet infected computers and clean them up using antivirus software. Fortinet's FortiClient can be used to scan and remove botnets from the infected hosts.

Malicious Websites Detected (1,087)

Malicious websites are sites known to host software/malware that is designed to covertly collect information, damage the host computer or otherwise manipulate the target machine without the user's consent. Generally visiting a malicious website is a precursor to infection and represents the initial stages of the kill chain. Blocking malicious sites and/or instructing employees not to visit/install software from unknown websites is the best form of prevention here.

Phishing Websites Detected (128)

Similar to malicious websites, phishing websites emulate the webpages of legitimate websites in an effort to collect personal or private (logins, passwords, etc.) information from end users. Phishing websites are often linked to within unsolicited emails sent to your employees. A skeptical approach to emails asking for personal information and hovering over links to determine validity can prevent most phishing attacks.

Proxy Applications Detected (39)

These applications are used (usually intentionally) to bypass in-place security measures. For instance, users may circumvent the firewall by disguising or encrypting external communications. In many cases, this can be considered a willful act and a violation of corporate use policies.

Remote Access Applications Detected (17)

Remote access applications are often used to access internal hosts remotely, thus bypassing NAT or providing a secondary access path (backdoor) to internal hosts. In the worst case scenario, remote access can be used to facilitate data exfiltration and corporate espionage activity. Many times, the use of remote access is unrestricted and internal corporate use changes should be put into practice.

P2P and Filesharing Applications (22)

These applications can be used to bypass existing content controls and lead to unauthorized data transfer and data policy violations. Policies on appropriate use of these applications need to be implemented.

Security and Threat Prevention

High Risk Applications

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy. Applications listed below were assigned a risk rating of 4 or higher.

High Risk Applications





















#	Risk	Application Name	Category	Technology	User	Bandwidth	Sessions
1	5	 Proxy.HTTP	 Proxy	Network-Protocol	335	24.30 GB	80,613
2	5	 TunnelBear	 Proxy	Client-Server	45	71.51 MB	5,821
3	5	 Hola.Unblocker	 Proxy	Client-Server	35	153.12 MB	5,553
4	5	 Tor	 Proxy	Client-Server	173	2.68 GB	1,882
5	5	 Private.Tunnel	 Proxy	Client-Server	84	17.54 MB	1,208
6	5	 Freegate.Searching	 Proxy	Client-Server	12	11.48 MB	1,083
7	5	 Proxy.Websites	 Proxy	Browser-Based	113	23.54 MB	827
8	5	 ZenMate	 Proxy	Browser-Based	19	62.61 MB	725
9	5	 Freedom	 Proxy	Client-Server	84	21.30 GB	445
10	5	 Psiphon	 Proxy	Client-Server	25	5.39 MB	380

Figure 1: Highest risk applications sorted by risk and sessions

Application Vulnerability Exploits

Application vulnerabilities can be exploited to compromise the security of your network. The FortiGuard research team analyzes these vulnerabilities and then develops signatures to detect them. FortiGuard currently leverages a database of more than 5,800 known application threats to detect attacks that evade traditional firewall systems. For more information on application vulnerabilities, please refer to FortiGuard at: <http://www.fortiguards.com/intrusion>.

Top Application Vulnerability Exploits Detected











#	Severity	Threat Name	Type	Victim	Source	Count
1	5	 Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	30	8	3,537
2	5	 Cisco.IOS.HTTP.Command.Execution	Improper Authentication	6	8	1,491
3	5	 Apache.Struts.REST.Plugin.Remote.Code.Execution	Code Injection	6	1	214
4	5	 MS.IIS.WebHits.Authentication.Bypass	Improper Authentication	2	1	136
5	5	 VxWorks.WDB.Agent.Debug.Service.Code.Execution	Permission/Privilege/Access Control	46	2	128
6	5	 Joomla.list.select.Parameter.SQL.Injection	Permission/Privilege/Access Control	31	3	58
7	5	 HTTP.Chunk.Overflow	Numeric Errors	2	4	35
8	5	 Joomla.Core.Session.Remote.Code.Execution	Code Injection	31	3	33
9	5	 Adobe.Flash.Player.JPEG.SOS.Memory.Corruption	Permission/Privilege/Access Control	1	1	32
10	5	 Cisco.Command.Execution	Permission/Privilege/Access Control	5	5	30

Figure 2: Top vulnerabilities identified, sorted by severity and count

Malware, Botnets and Spyware/Adware

There are numerous channels that cybercriminals use to distribute malware. Most common methods motivate users to open an infected file in an email attachment, download an infected file, or click on a link leading to a malicious site. During the security assessment, Fortinet identified a number of malware and botnet-related events which indicate malicious file downloads or connections to botnet command and control sites.

Top Malware, Botnets and Spyware/Adware Detected

#	Malware Name	Type	Application	Victim	Source	Count
1	HTML/Refresh.BC!tr	Virus	HTTP	5	16	292
2	WM/Agent.AN!tr	Virus	HTTP	3	31	45
3	Riskware/Mimikatz	Spyware	HTTP	4	31	42
4	EICAR_TEST_FILE	Virus	HTTP	3	7	36
5	JS/Moat.3B45BB5E!tr	Virus	HTTP	4	26	36
6	Malware_Generic.P0	Virus	HTTP	5	26	33
7	WM/Agent.BEA!tr	Virus	HTTP	2	19	28
8	W32/Agent.XRR!tr	Virus	HTTP	2	17	26
9	Andromeda.Botnet	Botnet C&C	Andromeda.Botnet	1	1	26
10	y,89.2	Virus		2	4	20

Figure 3: Common Malware, Botnets, Spyware and Adware detected

At-Risk Devices and Hosts

Based on the types of activity exhibited by an individual host, we can approximate the trustworthiness of each individual client. This client reputation is based on key factors such as websites browsed, applications used and inbound/outbound destinations utilized. Ultimately, we can create an overall threat score by looking at the aggregated activity used by each individual host.

Most At-Risk Devices and Hosts

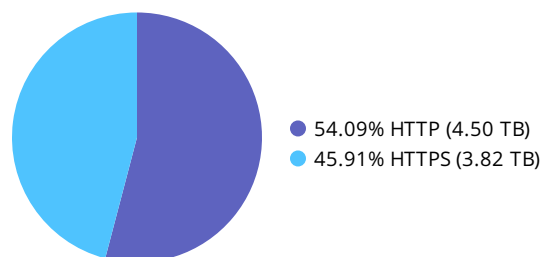
#	Device	Scores
1	10.168.1.10	25,521,535
2	172.16.57.2	19,364,400
3	10.10.30.115	15,417,765
4	10.15.148.2	10,191,520
5	172.16.19.7	9,071,265
6	10.10.30.4	8,702,360
7	172.16.100.56	6,244,250
8	10.15.251.7	5,989,705
9	172.16.4.2	5,827,280
10	172.16.61.6	3,593,525

Figure 4: These devices should be audited for malware and intrusion susceptibility

Encrypted Web Traffic

From a security perspective, it's important to visualize how much of your web-based traffic is encrypted. Encrypted traffic poses very real challenges for enterprises who want to ensure that those same applications are not being used for malicious purposes, including data exfiltration. Ideally, your firewall can inspect encrypted traffic at high speeds - this is why performance and hardware/ASIC offloading are key when evaluating a firewall.

HTTPS vs. HTTP Traffic Ratio



Top Source Countries

By looking at IP source traffic, we can determine the originating country of any particular request. Certain botnets, command and control functions, and even remote access can be session heavy and indicative of targeted attacks or persistent threats from nation-states. This chart is representative of country-based traffic - activity from specific originating nations may be anomalous and warrant further investigation.

Top Source Countries

#	Country	Bandwidth
1	United States	3.24 GB
2	Sweden	109.05 MB
3	Canada	29.70 MB
4	India	29.05 MB
5	China	28.52 MB
6	Japan	24.93 MB
7	United Kingdom	23.40 MB
8	Malaysia	22.92 MB
9	Israel	21.46 MB
10	Germany	17.57 MB

Figure 5: Activity originating from these countries should be audited for expected traffic sources

User Productivity

Application Usage

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application control. FortiGuard maintains thousands of application sensors and can even perform deep application inspection. For example, IT managers can get unprecedented visibility into filenames sent to the cloud or the titles of videos being streamed.

For application category details, see:

<http://www.fortiguards.com/encyclopedia/application>

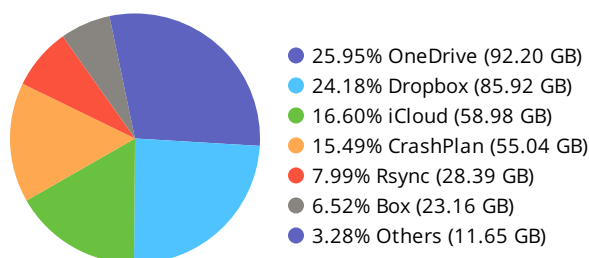
App Categories

Web.Others	25.57%
Network.Service	14.67%
Update	11.18%
General.Interest	10.16%
Collaboration	7.67%
Video/Audio	7.43%
Unknown	7.09%
Storage.Backup	5.03%
Proxy	4.38%
P2P	2.04%
Others	4.77%



With the proliferation of cloud-based computing, enterprises are increasingly reliant on third parties for infrastructure plumbing. Unfortunately for enterprises, this means that their information is only as secure as the cloud provider's security. In addition, it can often introduce redundancy (if services are already available internally) and increase costs (if not monitored properly).

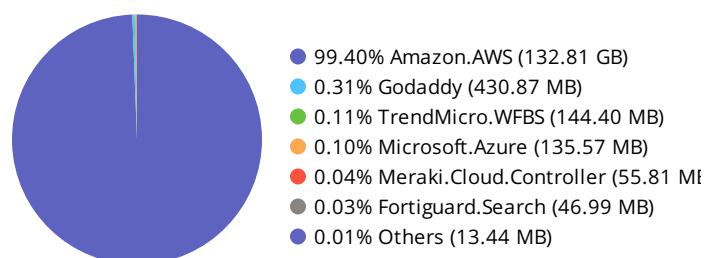
Cloud Usage (SaaS)



IT managers are often unaware of how many cloud-based services are in use within their organization. Sometimes, these applications can be used to circumvent or even replace corporate infrastructure already available to users in lieu of ease of use. Unfortunately, a potential side effect of this is that your sensitive corporate information could be transferred to the cloud. Accordingly, your data could be exposed if the cloud provider's security infrastructure is breached.

The adoption of "infrastructure as a service" (IaaS) platforms is popular and can be very useful when compute resources are limited or have specialized requirements. That said, the effective outsourcing of your infrastructure must be well regulated to prevent misuse. The occasional auditing of IaaS applications can be a useful exercise not only for security purposes, but also to minimize organizational costs associated with pay per use models or recurring subscription fees.

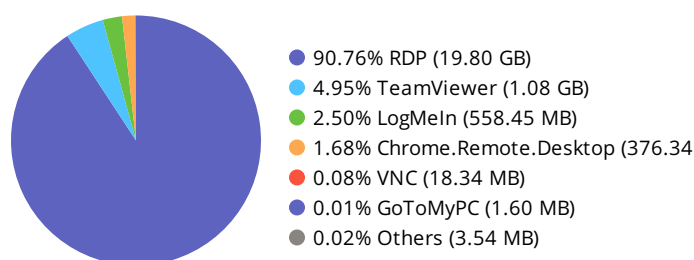
Cloud Usage (IaaS)



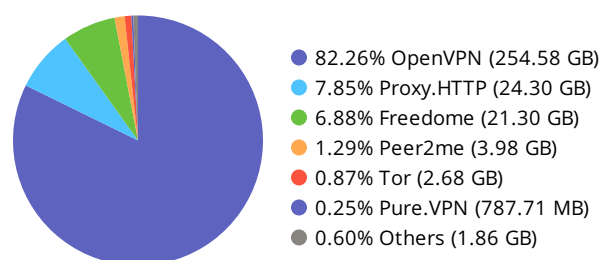
Application Category Breakdowns

Understanding application subcategories can give invaluable insights into how efficiently your corporate network is operating. Certain application types (such as P2P or gaming applications) are not necessarily conducive to corporate environments and can be blocked or limited in their scope. Other applications may have dual purpose uses (such as video/audio streaming or social media apps) and can be managed accordingly. These charts illustrate application categories sorted by the amount of bandwidth they used during the discovery period.

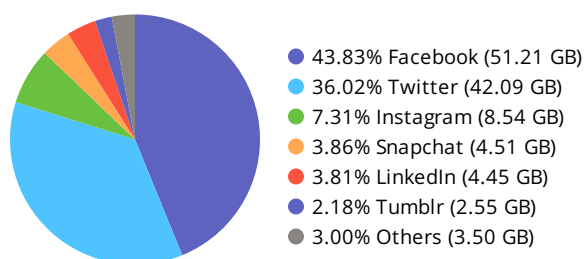
Remote Access Applications



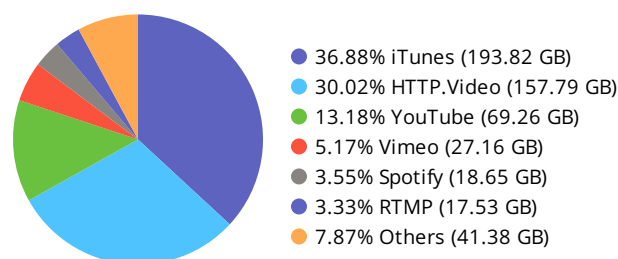
Proxy Applications



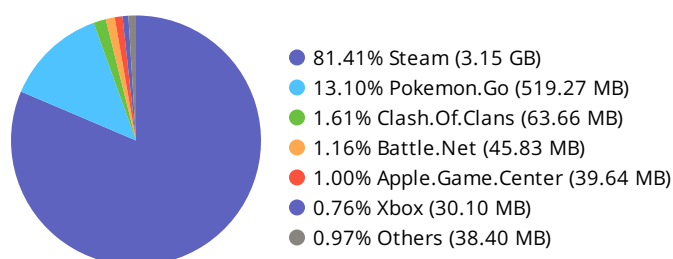
Top Social Media Applications



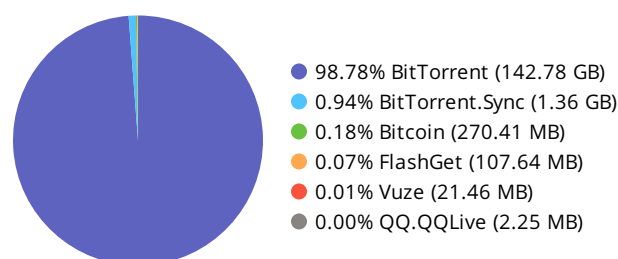
Top Video/Audio Streaming Applications



Top Gaming Applications













Top Peer to Peer Applications



Web Usage

Web 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.

Top Web Categories

#	URL Category	User	Count	Bandwidth
1	 Information Technology	5,292	3,188,205	856.45 GB
2	 Advertising	3,720	1,586,877	22.90 GB
3	 Search Engines and Portals	4,669	700,165	213.63 GB
4	 Business	3,822	612,444	25.19 GB
5	 Content Servers	4,327	516,564	70.19 GB
6	 Unrated	2,299	391,111	2.06 GB
7	 Meaningless Content	3,295	355,657	30.67 GB
8	 News and Media	2,665	329,175	11.85 GB
9	 Social Networking	3,548	152,757	5.91 GB
10	 Web Hosting	3,283	117,895	19.75 GB

In today's network environments, many applications leverage HTTP for communications – even some you wouldn't normally expect. The primary benefit of HTTP is that communication is ubiquitous, universally accepted and (generally) open on most firewalls. For most business-related and whitelisted applications this typically augments communication, but some non-business applications also use HTTP in either unproductive or potentially nefarious ways.











Top Web Applications

#	Application	Sessions	Bandwidth
1	HTTP	7,928,889	1.72 TB
2	HTTPS	10,408,546	1.54 TB
3	HTTPS.BROWSER	7,470,405	992.68 GB
4	HTTP.BROWSER	6,348,252	801.42 GB
5	MS.Windows.Update	86,382	470.58 GB
6	Microsoft.Portal	502,735	304.14 GB
7	Apple.Services	114,759	221.32 GB
8	Google.Services	779,255	216.51 GB
9	iTunes	9,528	193.82 GB
10	HTTP.Video	29,684	157.78 GB

Websites Frequented











Websites browsed are strong indicators of how employees utilizing corporate resources and how applications communicate with specific websites. Analyzing domains accessed can lead to changes in corporate infrastructure such as website blocking, deep application inspection of cloud-based apps and implementation of web traffic acceleration technologies.

Most Visited Web Domains

#	Domain	Category	Visits
1	vid-io.springserve.com	 Advertising	417,155
2	officecdn.microsoft.com	 Information Technology	370,453
3	ads.adaptv.advertising.com	 Advertising	356,693
4	www.google.com	 Search Engines and Portals	258,835
5	www.hybrik.com	 Information Technology	251,046
6	api.simple.chat	 Information Technology	226,744
7	safebrowsing-cache.google.com	 Search Engines and Portals	223,213
8	fqsvr.fortinet.net	 Information Technology	219,162
9	8.8.8.8.in-addr.arpa	 Unrated	206,327
10	ib.adnxs.com	 Advertising	202,453

Estimated browsing times for individual websites can be useful when trying to get an accurate picture of popular websites. Typically, these represent internal web resources such as intranets, but they can occasionally be indicative of excessive behavior. Browse times can be employed to justify the implementation of web caching technologies or help shape organizational corporate use policies.

Top Websites by Browsing Time

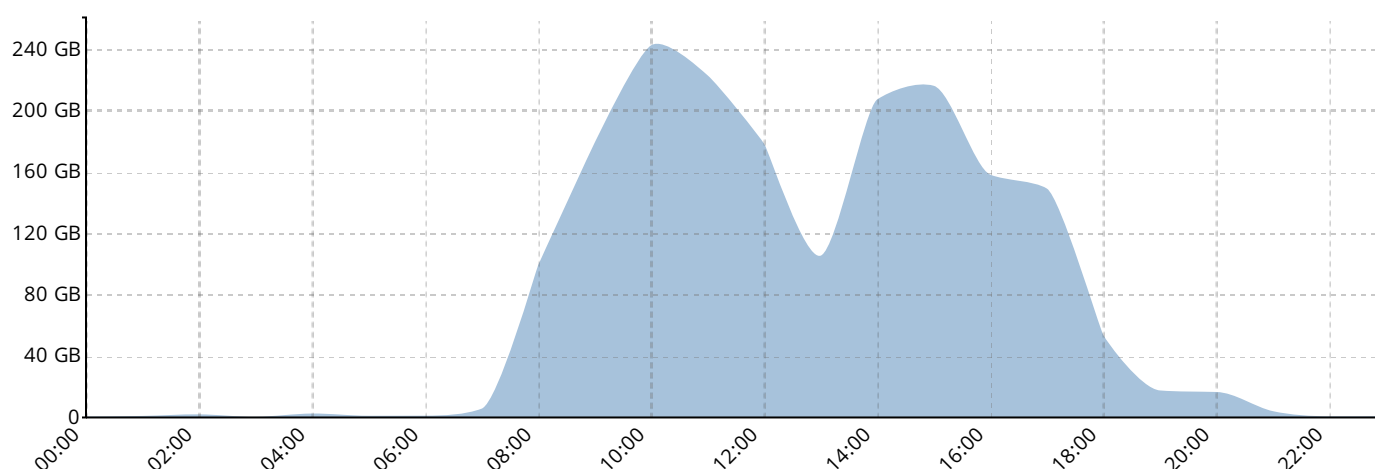
#	Sites	Category	Browsing Time (hh:mm:ss)
1	ssw.live.com	 Search Engines and Portals	317:40:16
2	cdn.content.prod.cms.msn.com	 Search Engines and Portals	297:56:34
3	ping.chartbeat.net	 Information Technology	149:55:39
4	clients1.google.com	 Search Engines and Portals	115:40:13
5	ocsp.digicert.com	 Information Technology	115:26:17
6	tile-service.weather.microsoft.com	 Information Technology	96:06:20
7	push.bitdefender.net	 Information Technology, Information and Computer Security, Web Hosting	84:07:09
8	www.microsoft.com	 Information Technology, Information and Computer Security	79:32:31
9	crl.microsoft.com	 Information Technology, Shopping, Web Hosting	70:15:55
10	download.cdn.mozilla.net	 Information Technology	69:37:54

Network Utilization

Bandwidth

By looking at bandwidth usage when distributed over an average day, administrators can better understand their organizational ISP connection and interface speed requirements. Bandwidth can also be optimized on an application basis (using throttling), specific users can be prioritized during peak traffic times, and updates can be rescheduled outside of working hours.

Average Bandwidth by Hour



One of the most telling ways to analyze bandwidth is by looking at destinations and sources generating the most traffic. Common destination sites (e.g. external websites), such as those for OS/firmware updates, can be throttled to allow prioritized, business critical traffic. Internally, high traffic hosts can be optimized through traffic shaping or corporate use policies.

Top Bandwidth Consuming Sources/Destinations

#	Host Name	Bandwidth
1	tlu.dl.delivery.mp.microsoft.com	130.51 GB
2	au.v4.download.windowsupdate.com	116.17 GB
3	iosapps.itunes.apple.com	113.30 GB
4	au.download.windowsupdate.com	97.31 GB
5	officecdn.microsoft.com	89.91 GB
6	swcdn.apple.com	69.34 GB
7	archive-7.kali.org	65.93 GB
8	us-ore-00001.s3.amazonaws.com	61.92 GB
9	usdal-edge.icloud-content.com	44.67 GB
10	officecdn.microsoft.com.edgesuite.net	23.20 GB

FortiGuard Security and Services

Knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation for providing effective security. Hundreds of researchers at FortiGuard Labs scour the cyber landscape every day to discover emerging threats and develop effective countermeasures to protect organizations around the world. They are the reason FortiGuard is credited with over 250 zero-day and vulnerability discoveries and why Fortinet security solutions score so high in real-world security effectiveness tests at NSS Labs, Virus Bulletin, AV Comparatives, and more.



Next Generation Application Control & IPS

Application control and intrusion prevention (IPS) are foundational security technologies in a next generation firewall like the FortiGate. Organizations worldwide use FortiGuard application control and IPS in the FortiGate platform to manage their applications and block network intrusions (every minute of every day FortiGuard blocks ~470,000 intrusion attempts). FortiGates running application control and IPS are tested for effectiveness in industry comparison tests by NSS Labs and consistently receive Recommended ratings.



Web Filtering

Every minute of every day FortiGuard Labs processes approximately 43M URL categorization requests and blocks 160k malicious websites. The Web Filtering service rates over 250M websites and delivers nearly 1.5M new URL ratings every week. FortiGuard is the only VBWeb certified web filtering solution - blocking 97.7% of direct malware downloads in 2016 tests.



AntiVirus and Mobile Security

Every minute of every day FortiGuard Labs neutralizes approximately 95,000 malware programs targeting traditional, mobile and IoT platforms. Patented technologies enable FortiGuard antivirus to identify thousands of current and future malware variants with a single signature – optimizing both security effectiveness and performance. Fortinet consistently receives superior effectiveness results in industry testing with Virus Bulletin and AV Comparatives



AntiSpam

Every minute of every day FortiGuard Labs blocks approximately 21,000 spam emails and each week the Labs deliver approximately 46M new and updated spam rules. Email is the #1 vector for the start of an advanced attack on an organization so highly effective antispam is a key part of a security strategy.



Advanced Threat Protection (FortiSandbox)

Thousands of organizations around the world leverage FortiSandbox to identify advanced threats. FortiSandbox consistently receives a Recommended rating for breach detection systems from NSS Labs in industry tests and in 2015 NSS Labs tests achieved a 97%+ breach detection rating.



IP Reputation

Every minute of every day FortiGuard Labs blocks approximately 32,000 botnet command & control communication attempts. A key part of the attack kill chain on an organization is when the threat communicates with a command & control server – either to download additional threats or to exfiltrate stolen data. IP and Domain address reputation blocks this communication, neutralizing threats.