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: Informata College

Location: San Francisco, CA, US

Industry: Education
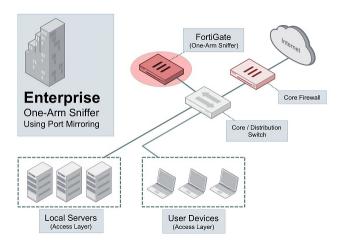
Company Size: 1,000-2,499 employees

Test Details

Test Start Date: Feb 14, 2018

FortiGate Model: FG-300D

Network Analyzed: Internal LAN

Test Duration: 4 Day(s)

FortiOS Firmware: FortiOS 5.6.2

Functions Enabled: Firewall + Sandbox

Deployment and Methodology

Your network was monitored with a FG-300D in One Arm Sniffer 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

SECURITY AND THREAT PREVENTION

IPS Attacks Detected: 2,013

High-Risk Applications Used: 16

Malware/Botnets Detected: 7

Malicious Websites Detected: 123

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.

USER PRODUCTIVITY

Applications Detected: 329

Top Application Category: Network.Service

Top Website: cdn.speedshiftmedia.com

Top Used Application: SSL

Websites Visited: 69

Top Web Category: Advertising

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.

NETWORK UTILIZATION

Total Bandwidth: 22.62 GB

Highest Session Host: 172.18.58.121

Top Host by Bandwidth: 172.16.116.100

Average Log Rate/Sec: 11.40

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.

Industry Comparables

Industry: Education

As ever-increasing numbers of devices are brought to campuses by students, faculty and administrators, schools need to scale their networks for access while providing additional security to protect sensitive information, as well as to meet compliance standards like CIPA, FERPA, and COPPA. Educational institutions need the latest in network security and access technologies; however, limited budgets often force IT organizations to make hard choices between the two.

In the charts below, the term "company" refers to your organization. This activity gives you an idea of where you stand relative to other organizations in your specific industry. By using similar organizations as a baseline, some progressive companies continually optimize their network to target "above industry average" security practices.

IPS Attacks per Day

#	Entity	Count
1	Company	503
2	Industry	20,807
3	Overall	18,859

Evasive Apps per Day

#	Entity	Count
1	Company	0
2	Industry	2
3	Overall	1

Top Malware (Company)

#	Malware Name	Type	Application
1	W32/Generic.AC.3396208	Virus	HTTP
2	Adware/StartSurf	Adware	HTTP
3	W32/Agent.WCT!tr.bdr	Virus	HTTP
4	W32/InstallCore_ACY.GEN	Virus	HTTP
5	W32/KeyLogger.AUVU!tr	Virus	HTTP

Top Malware (Industry)

#	Malware Name	Type	Application
1	H-worm.Botnet	Botnet C&C	H-worm.Botnet
2	Zeroaccess.Botnet	Botnet C&C	Zeroaccess.Botnet
3	Andromeda.Botnet	Botnet C&C	Andromeda.Botnet
4	Expiro.Botnet	Botnet C&C	Expiro.Botnet
5	Conficker.Botnet	Botnet C&C	Conficker.Botnet

HTTPS vs. HTTP Usage

#	Entity	Percentage
1	Company	112.48%
2	Industry	108%
3	Overall	106%

Cloud Usage (IaaS + SaaS Apps)

#	Entity	Count
1	Company	51
2	Industry	50,465
3	Overall	295,046

Sandbox Analysis

Today's increasingly sophisticated threats can mask their maliciousness and bypass traditional antimalware security. Conventional antimalware engines are, in the time afforded and to the certainty required, often unable to classify certain payloads as either good or bad; in fact, their intent is unknown. Sandboxing helps solve this problem – it entices unknown files to execute in a protected environment, observes its resultant behavior and classifies its risk based on that behavior. With this functionality enabled for your assessment, we have taken a closer look at files traversing your network.
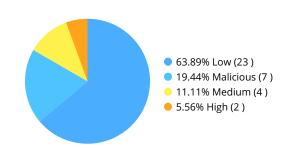
Results of Sandbox Analysis

Total Files Analyzed (8,190)
After a standard anti-malware check on the FortiGate, select files were sent to the sandbox for further inspection. The number here represents the total number of files that were executed in a protected environment while individual behaviors were observed (such as registry updates, file deletions, or attempts to communicate with external websites).

The results of behavioral analysis are usually categorized in one of three ways: clean, suspicious, or malicious. A designation of clean means that no abnormal behaviors were observed and the file can be considered safe. Suspicious activities are potentially dangerous and may warrant further attention – for instance, a high suspicion file may try to replicate itself whereas a low suspicion file may only create abnormal registry settings. A malicious designation should be considered a legitimate threat to your network and requires immediate attention. The chart rendered here shows malicious and suspicious files (e.g. it does not include files designated as clean).

Malicious and Suspicious Files

- 63.89% Low (23)
- 19.44% Malicious (7)
- 11.11% Medium (4)
- 5.56% High (2)

#	Filename	Service	Risk	Suspicious Behaviors	Count
1	1D26B266.vXE	HTTP	Malicious	Threat_Intelligence The executable tries to inject a PE image to other processess Executable deleted itself after execution Executable dropped a copy of itself This file checked registry for anti-virtualization or anti-debug This file checked devices for anti-virtualization or anti-debug	1
2	1D28E4E7.vsc	HTTP	Malicious	Threat_Intelligence	1
3	1D43634F.vsc	HTTP	Malicious	This file checked registry for anti-virtualization or anti-debug This file checked devices for anti-virtualization or anti-debug	1
4	1D45FCB7.vsc	HTTP	Malicious	Executable deleted itself after execution Executable dropped a copy of itself Threat_Intelligence	1
5	1D46A1FA.vsc	HTTP	Malicious	The executable tries to inject a PE image to other processess	1

Recommended Actions

Application Vulnerability Attacks Detected (15)
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 (7)
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 (0)
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 (123)
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 (1)
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 (5)
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 (5)
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 (5)
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.
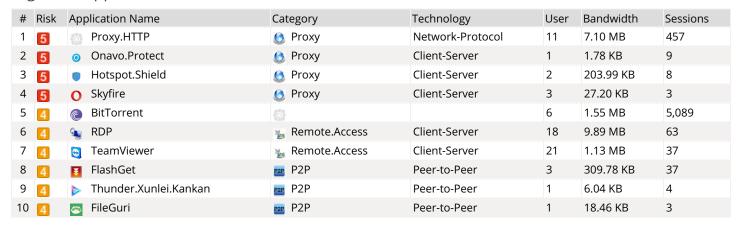
High Risk Applications

#	Risk	Application Name	Category	Technology	User	Bandwidth	Sessions
1	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
2	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
3	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
4	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
5	4	BitTorrent			6	1.55 MB	5,089
6	4	RDP	Remote.Access	Client-Server	18	9.89 MB	63
7	4	TeamViewer	Remote.Access	Client-Server	21	1.13 MB	37
8	4	FlashGet	P2P	Peer-to-Peer	3	309.78 KB	37
9	4	Thunder.Xunlei.Kankan	P2P	Peer-to-Peer	1	6.04 KB	4
10	4	FileGuri	P2P	Peer-to-Peer	1	18.46 KB	3

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.fortiguard.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	8	3	15
2	5	MS.GDIPlus.JPEG.Buffer.Overflow	Buffer Errors	3	2	10
3	5	MS.IE.MSXML.Object.Handling.Code.Execution	Buffer Errors	1	1	2
4	5	McAfee.Web.Reporter.EJBInvokerServlet.Object.Code.Execution	Code Injection	1	1	1
5	4	MS.Windows.ASN.1.Bitstring.Heap.Overflow	Buffer Errors	1	1	1
6	4	MS.Windows.ASN.1.Bitstring.Overflow	Buffer Errors	1	1	1
7	4	NBSS.ASN1.Bitstring.Heap.Overflow	Buffer Errors	1	1	1
8	4	OpenSSL.ChangeCipherSpec.Injection	Information Disclosure	1	1	1
9	2	MSSQL.Login.Brute.Force	Anomaly	1	5	395
10	2	IMAP.Unknown.Reply	Anomaly	1	1	42

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	W32/Generic.AC.3396208	Virus	HTTP	1	1	6
2	Riskware/ProductKey	Spyware	HTTP	1	1	1
3	W32/Agent.WCT!tr.bdr	Virus	HTTP	1	1	1
4	Adware/StartSurf	Adware	HTTP	1	1	1
5	W32/InstallCore_ACY.GEN	Virus	HTTP	1	1	1
6	W32/KeyLogger.AUVU!tr	Virus	HTTP	1	1	1
7	W32/Malware_fam.NB	Virus	HTTP	1	1	1

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.
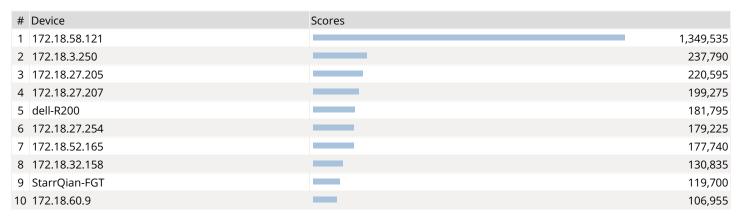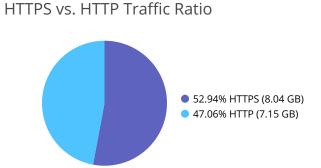
Most At-Risk Devices and Hosts

#	Device	Scores	
1	172.18.58.121		1,349,535
2	172.18.3.250		237,790
3	172.18.27.205		220,595
4	172.18.27.207		199,275
5	dell-R200		181,795
6	172.18.27.254		179,225
7	172.18.52.165		177,740
8	172.18.32.158		130,835
9	StarrQian-FGT		119,700
10	172.18.60.9		106,955

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

- 52.94% HTTPS (8.04 GB)
- 47.06% HTTP (7.15 GB)

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	213.31 MB
2	Anonymous Proxy	7.73 MB
3	🇬🇧 United Kingdom	4.13 MB
4	🇧🇪 Belgium	1.51 MB
5	🇳🇱 Netherlands	603.07 KB
6	🇮🇪 Ireland	389.32 KB
7	🇷🇴 Romania	47.75 KB
8	🇷🇺 Russian Federation	37.82 KB
9	🇫🇷 France	26.88 KB
10	🇨🇳 China	4.12 KB

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:
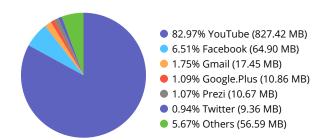http://www.fortiguard.com/encyclopedia/application

App Categories

Category	%
●Network.Service	49.73%
●Web.Client	12.27%
●Web.Others	11.09%
●Video/Audio	9.10%
●Unknown	7.11%
●General.Interest	4.77%
●Collaboration	2.30%
●Update	2.17%
●Email	0.66%
●Social.Media	0.55%
●Others	0.25%

App Categories

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).
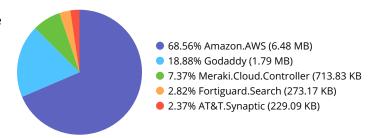
Cloud Usage (SaaS)

- ● 82.97% YouTube (827.42 MB)
- ● 6.51% Facebook (64.90 MB)
- ● 1.75% Gmail (17.45 MB)
- ● 1.09% Google.Plus (10.86 MB)
- ● 1.07% Prezi (10.67 MB)
- ● 0.94% Twitter (9.36 MB)
- ● 5.67% Others (56.59 MB)

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)

- ● 68.56% Amazon.AWS (6.48 MB)
- ● 18.88% Godaddy (1.79 MB)
- ● 7.37% Meraki.Cloud.Controller (713.83 KB
- ● 2.82% Fortiguard.Search (273.17 KB)
- ● 2.37% AT&T.Synaptic (229.09 KB)
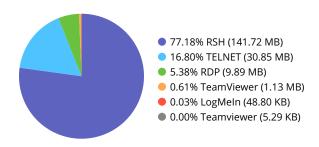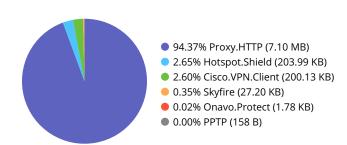
Application Category Breakdowns

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.
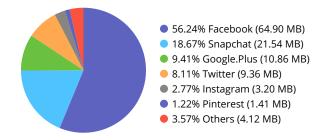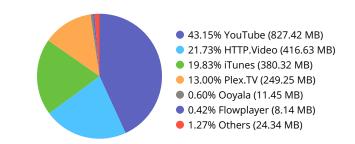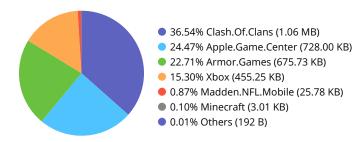
Remote Access Applications

- 77.18% RSH (141.72 MB)
- 16.80% TELNET (30.85 MB)
- 5.38% RDP (9.89 MB)
- 0.61% TeamViewer (1.13 MB)
- 0.03% LogMeIn (48.80 KB)
- 0.00% Teamviewer (5.29 KB)

Proxy Applications

- 94.37% Proxy.HTTP (7.10 MB)
- 2.65% Hotspot.Shield (203.99 KB)
- 2.60% Cisco.VPN.Client (200.13 KB)
- 0.35% Skyfire (27.20 KB)
- 0.02% Onavo.Protect (1.78 KB)
- 0.00% PPTP (158 B)

Top Social Media Applications

- 56.24% Facebook (64.90 MB)
- 18.67% Snapchat (21.54 MB)
- 9.41% Google.Plus (10.86 MB)
- 8.11% Twitter (9.36 MB)
- 2.77% Instagram (3.20 MB)
- 1.22% Pinterest (1.41 MB)
- 3.57% Others (4.12 MB)

Top Video/Audio Streaming Applications

- 43.15% YouTube (827.42 MB)
- 21.73% HTTP.Video (416.63 MB)
- 19.83% iTunes (380.32 MB)
- 13.00% Plex.TV (249.25 MB)
- 0.60% Ooyala (11.45 MB)
- 0.42% Flowplayer (8.14 MB)
- 1.27% Others (24.34 MB)

Top Gaming Applications

- 36.54% Clash.Of.Clans (1.06 MB)
- 24.47% Apple.Game.Center (728.00 KB)
- 22.71% Armor.Games (675.73 KB)
- 15.30% Xbox (455.25 KB)
- 0.87% Madden.NFL.Mobile (25.78 KB)
- 0.10% Minecraft (3.01 KB)
- 0.01% Others (192 B)

Top Peer to Peer Applications

- 84.24% Raysource (1.75 MB)
- 14.60% FlashGet (309.78 KB)
- 0.87% FileGuri (18.46 KB)
- 0.28% Thunder.Xunlei.Kankan (6.04 KB)

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	2	180	1.04 MB
2	Search Engines and Portals	2	53	32.84 MB
3	Armed Forces	1	42	576.42 KB
4	Advertising	1	34	1.68 MB
5	Web Hosting	2	9	217.53 KB
6	Content Servers	1	9	38.69 KB
7	Pornography	1	8	30.30 KB
8	Finance and Banking	1	7	67.70 KB
9	Business	1	6	13.58 KB
10	Reference	1	4	38.08 MB

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

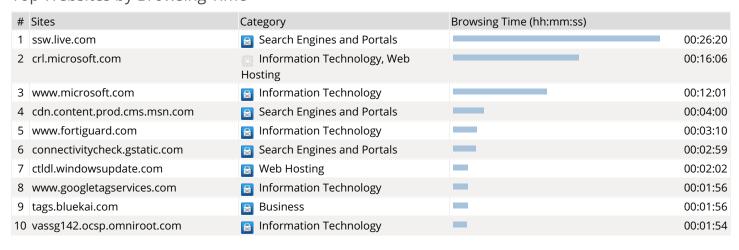| #	Application	Sessions	Bandwidth
1	SSL	129,754	6.28 GB
2	HTTP.BROWSER	223,132	4.41 GB
3	YouTube	4,139	806.89 MB
4	HTTP.Audio	532	507.46 MB
5	HTTP.Video	298	415.62 MB
6	iTunes	180	380.32 MB
7	HTTPS.BROWSER	7,338	372.21 MB
8	Apple.Services	25	241.61 MB
9	HTTP.Segmented.Download	181	236.50 MB
10	MS.Office.Live	1,050	182.07 MB

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	cdn.speedshiftmedia.com	📗 Advertising	335
2	www.fortiguard.com	📘 Information Technology	91
3	adserving.speedshiftmedia.com	📗 Advertising	88
4	api.speedshiftmedia.com	📘 Business	52
5	googleads.g.doubleclick.net	📗 Advertising	48
6	www.google.com	📘 Search Engines and Portals	45
7	crl.microsoft.com	📘 Information Technology	45
8	bbs.wforum.com	📘 Armed Forces	42
9	pagead2.googlesyndication.com	📗 Advertising	39
10	tlu.dl.delivery.mp.microsoft.com	📘 Search Engines and Portals	39

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.
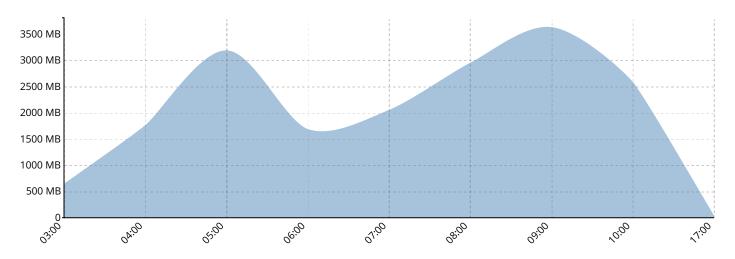
Top Websites by Browsing Time

#	Sites	Category	Browsing Time (hh:mm:ss)	
1	ssw.live.com	📘 Search Engines and Portals	▬▬▬▬▬▬▬▬▬	00:26:20
2	crl.microsoft.com	⚪ Information Technology, Web Hosting	▬▬▬▬▬▬	00:16:06
3	www.microsoft.com	📘 Information Technology	▬▬▬▬	00:12:01
4	cdn.content.prod.cms.msn.com	📘 Search Engines and Portals	▬▬	00:04:00
5	www.fortiguard.com	📘 Information Technology	▬	00:03:10
6	connectivitycheck.gstatic.com	📘 Search Engines and Portals	▬	00:02:59
7	ctldl.windowsupdate.com	📘 Web Hosting	▬	00:02:02
8	www.googletagservices.com	📘 Information Technology	▬	00:01:56
9	tags.bluekai.com	📘 Business	▬	00:01:56
10	vassg142.ocsp.omniroot.com	📘 Information Technology	▬	00:01:54

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

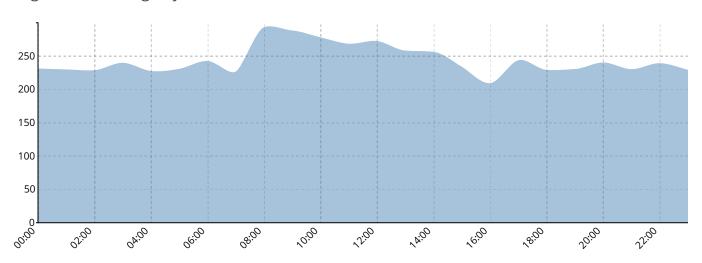| #	Host Name	Bandwidth	
1	ca.archive.ubuntu.com		38.08 MB
2	tlu.dl.delivery.mp.microsoft.com		32.57 MB
3	cdn.speedshiftmedia.com		1.41 MB
4	security.ubuntu.com		817.14 KB
5	bbs.wforum.com		576.42 KB
6	wiki.fortinet.com		244.14 KB
7	dl.delivery.mp.microsoft.com		158.24 KB
8	us-ads.openx.net		145.34 KB
9	www.fortiguard.com		77.32 KB
10	ssw.live.com		75.41 KB

Sizing Information

Understanding average log rates is extremely beneficial when sizing a security environment from a performance standpoint. Higher average log rates applied to specific hours usually indicate peak traffic usage and throughput. Calculating enterprise-wide log rates can also help when sizing for upstream logging/analytics devices such as FortiAnalyzer. Keep in mind, the log rates presented here are with the full logging capabilities of the FortiGate enabled and will include all log types (traffic, anti-virus, application, IPS, web and system events).

Average Log Rate by Hour

The average number of sessions invoked during an hour can be indicative of performance requirements (not only for FortiAnalyzer, but also for the final architected FortiGate solution). Generally, there is a correlation between throughput, log rates and session usage. Sessions are another data point that can be used to not only determine how to size the current network, but also futureproof the network for increased traffic speeds.
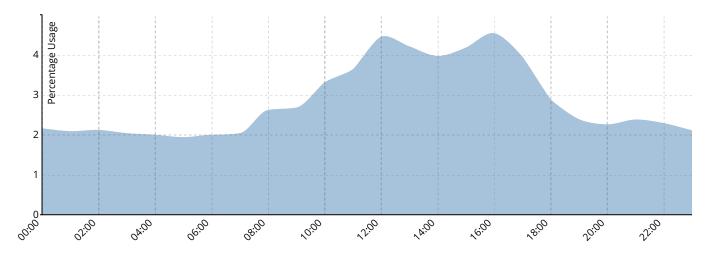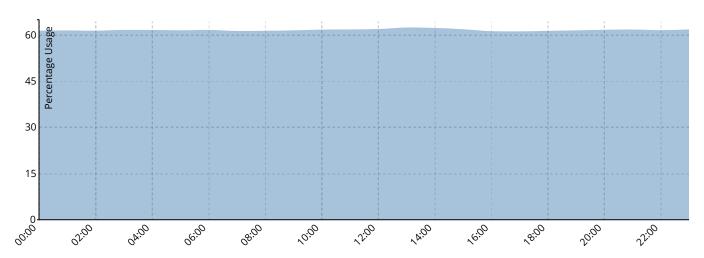
Average Session Usage by Hour

Firewall Statistics

CPU usage of a FortiGate is often used to size a final solution properly. By looking at an hourly breakdown of CPU utilization statistics, it's easy to get a good idea about how FortiGates will perform in the target network. Typically, with higher throughput, more logs are generated. If 75% or more utilization is sustained over a long period of time, either a more powerful model or revised architecture may be required for final implementation.

Average FortiGate CPU Usage by Hour

Similarly, memory usage over time is an indicator of the FortiGate's sustainability in the target network environment. Memory usage may remain high even when throughput is relatively low due to logging activity (or queued logging activity) over time.

Average FortiGate Memory Usage by Hour

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.